AMV BBDO

Employee Handbook

Introduction to the Handbook

This is the employee handbook (the "**Handbook**") of Abbott Mead Vickers Group Ltd (referred to hereafter as the "**Company**"). It contains a wide range of policy and other information relevant to you personally and to the Company's business operations. It is intended to be based upon UK and industry best practice and also to comply with the Company's commitments as part of the Omnicom Group and the BBDO Worldwide Network.

Many policies may apply to you even if you are not directly employed.

Therefore, for ease of reference, things that apply to everyone working at or on behalf of the Company are contained in Part A.

Part B is for employees only.

This handbook is not part of your contract of employment. It does not create any contractual rights or obligations, and may be amended by the Company at any time.

However, whilst the handbook does not create contractual rights or obligations, it forms the framework of best practice for all people working at the Company. Failure to follow the guidelines and practices contained herein may result, in the case of employees, in disciplinary action (up to and including summary dismissal) or, in the case of non-employees, termination of the relationship and/or legal action.

If you have any feedback or questions about the information included, please speak to the HR Department.

Table of Contents

Part A - For all people working at or on behalf of the Company

A.1 OMNICOM CODE OF BUSINESS CONDUCT

A1.1 Introduction to the Code of Conduct

This code of business conduct aims to ensure that we follow best practice in all our dealings, and that we act within the laws within the UK and also certain US laws because we are ultimately part of the Omnicom group. Our business conduct must among other things comply with US regulations relating to the Sarbanes-Oxley Act 2002, introduced as a result of the Enron and WorldCom scandals. It is in all our interests to be aware of ethical and business risks to prevent problems before they arise. No set of specific rules can anticipate or capture every possible instance in which an ethical issue may arise. Instead, all of us must be guided by the overarching principle that we are committed to fair and honest conduct and use our judgment and common sense whenever confronted with an ethical issue. Our reputation depends, to a very large measure, on you taking personal responsibility for maintaining and adhering to the policies and guidelines set out below.

A1.2 Conflicts of Interests

You must avoid situations where your personal interests interfere with the Company's interests. You must declare any actual or potential conflict of interest promptly in accordance with this policy. If in any doubt, you should discuss the matter with your manager, the Finance Director or Omnicom's Compliance Officer.

A1.3 No Insider Trading

You must not trade in Omnicom stock on the basis of material, non-public information concerning any Omnicom group company (which includes the Company), nor should you 'tip' others who could reasonably be expected to trade in Omnicom securities. Confidential information should not be shared with others, even with fellow employees or other individuals working at the Company unless they have a reasonable business reason to be aware of it. "**Material**" information is generally regarded as information that an investor would reasonably be expected to think is important in deciding whether to buy, hold or sell a security. In short, it is any information that could reasonably affect the price of the security. "**Non-public**" means information not available to the investing community or the public at large.

A1.4 Confidentiality Generally

You should maintain the confidentiality of information entrusted to you by the Company or its clients, except when disclosure is authorised or legally mandated. Confidential information includes proprietary information such as our plans, forecasts and employee information, as well as any other non-public information that might be of use to competitors or harmful to the Company and/or Omnicom Group or our clients if disclosed. It also includes information that others have entrusted to us on a confidential basis. Your obligations not to disclose confidential information continue even after employment ends.

You must keep all confidential information safe, including confidential information belonging to clients and other third parties, share it internally only on a 'need to know' basis, and only disclose it to third parties on a confidential basis and with appropriate authorisation to do so. You must not derive any personal advantage, or procure advantage for a third party, from information which is not generally available and which has been obtained by reason of, or in the course of your employment or engagement with the Company.

A1.5 Gifts and Hospitality

You owe a duty to advance the Company's and Omnicom Group's legitimate interests. You should not personally take investment or other corporate opportunities that become available to you, or family members, as a result of employment. The test for this is simple - don't take anything offered to you, including any loan or other financial benefit, on terms that would not be made available to you if you were not an employee of the Company or otherwise working at the Company. This does not, of course, prohibit customary business entertainment and non-cash gifts meant to create goodwill and sound working relationships consistent with customary business practice. We expect you to exercise good judgment and discretion in giving or accepting any gift.

Gifts of a value of more than £50 may not be given or accepted. You are required to inform the Finance Department of the receipt of all hospitality of a value of more than £200. Any gift or hospitality regardless of value that encourages you to favour the interests of the donor or any other third party over the Company's and Omnicom's interests must not be accepted. You must not accept or give any gift of cash or a cash equivalent. You must not offer, give or receive bribes or participate in any kind of corrupt activity, either directly or through any third party on the Company's or Omnicom Group's behalf.

Provided that there is no cause for improper influence on the performance of your duties, you may accept, but not solicit, from clients and service providers reasonable business entertainment, such as a meal and low value gifts given on a festive occasion in accordance with customary practice.

A1.6 Anti-Corruption and Bribery

The Company is committed to carrying out our business fairly, honestly and openly and adopts a zero tolerance approach towards bribery. Bribery is a criminal offence which can lead organisations to a significant fine and individuals up to 10 years in prison.

Bribery is where a person offers, promises, gives or receives from another person an advantage, whether financial or otherwise (for example, providing or receiving cash, gifts, hospitality, entertainment) intending that advantage to induce the person to perform a function or activity improperly, or as a reward for doing so.

It makes no difference whether the advantage is provided to or received from public officials, private individuals or companies. Bribes are against the law, no matter what the 'local custom' may be. Requesting or agreeing to accept or receive a bribe is also a crime.

Therefore, you must not offer, give or receive bribes or make or accept improper payments (including facilitation payments) to obtain new business, retain existing business, or secure any improper advantage, and you must not permit others to do such things for us.

The Company considers such conduct amounts to gross misconduct. Any bribery or other breaches of this policy may result in disciplinary action, leading to your dismissal without notice for employees or termination of your engagement.

We encourage you to be vigilant about any situations that could involve bribery, and particularly when you are dealing with situations where bribery or the opportunity for bribery is more likely to occur. You must not aid and abet others to give or receive bribes. Please report any bribery, attempts to bribe, or to solicit bribes from the Company, and any suspicions you have about bribery immediately to your manager, the Finance Director or Omnicom's Compliance Officer

A1.7 Competition and Fair Dealing

You have most likely signed agreements that subject you to non-competition restrictions, or prohibitions against soliciting customers or employees, any or all of which may apply even after termination of employment. As a matter of policy, the Company must vigorously enforce these kinds of limitations, whether they arise under employment agreements, stock award agreements, acquisition agreements or otherwise. We also must outperform our competitors through our innovation, execution and hard work, not through unethical or illegal business practices. Examples include theft of competitively sensitive information, and giving or receiving inappropriate gifts or other improper inducements that are not consistent with customary business practice. You must not take unfair advantage of anyone through manipulation, concealment, misrepresentation of material facts or any other unfair practice.

A1.8 Accounting and Record-Keeping

The Company requires honest and accurate recording and reporting of information in order to make responsible business decisions and accurately calculate our financial results. Unrecorded or 'off the books' funds or other assets, charges or obligations are strictly prohibited, as are special billing or payment procedures that suggest evasion of tax or other requirements by the other party to them.

A1.9 Protection and Proper Use of Assets

The misuse of Company assets is a disciplinary offence. Theft of; carelessness with; or the wasting of any Company property has a direct impact on profitability. All Company assets should therefore only be used for legitimate business purposes. If an employee is found (without consent) to be using these Company assets other than for legitimate business purposes, this will be considered to be misuse.

If an employee makes any purchase from a related party (for example: a family member, friend, previous associate, or prospective associate) for which they expect the Company to be responsible, then they will need to be able to clearly demonstrate that the transaction is in the best interests of the Company. If in doubt, the employee should seek prior written approval for any such transaction. If it cannot be proven to the satisfaction of the Company that such a transaction is in the best interests of the Company, and there is no prior written approval, this will be considered to be a misuse of Company assets.

A1.10 Political Activities

Any decision to become involved in political activities is entirely personal and voluntary, and Company funds should therefore not be used for contributions to any political party or candidates seeking election. Omnicom recognise your right and responsibility to lobby on behalf of issues that affect the Company and business operations, but only in full compliance with the laws and regulations governing these activities.

A1.11 Implementation and Enforcement

Acts that violate these policies may be considered a breach of your terms and conditions of employment and may result in disciplinary action and legal sanctions being taken against you, including where appropriate the immediate termination of employment. If you have any doubts about whether you or anyone else is adhering to these principles, you should feel free to discuss the matter with your manager, the Finance Director or Omnicom's compliance office. If you feel uncomfortable about doing that and wish to remain anonymous, you can use the mechanism we have developed for confidentially reporting possible violations of this policy or other improper behaviour. Details for contacting Omnicom's compliance office can be found on the websites of Omnicom and each of its networks should you wish to make a report. All reports of possible violations of which management becomes aware will be promptly considered. Omnicom will not punish any employee or other individual working at the Company for making any report in good faith.

A1.12 Waivers

Under applicable requirements, only the Governance Committee of Omnicom’s Board of Directors is permitted to waive a provision of these policies for Omnicom’s Executive Officer or Directors, and we cannot foresee circumstances in which any such waiver would be granted. Waivers for any other employee or other individual working at the Company may be made only by an appropriate Company officer or Director, and would only be made under exceptional circumstances.

A.2 DOCUMENT RETENTION IN THE EVENT OF AN INVESTIGATION

A2.1 Reasons for these Guidelines

The Company is obliged to comply with UK and US laws with regard to retaining certain documentation in the event of any serious investigations or litigation. The Omnicom Document Retention Guidelines are outlined below in some detail to ensure you understand and are clear on your obligations in this area. Please be aware that as a result of the Enron and WorldCom scandal and the new legislation that followed, document retention is a particularly sensitive area for any company that is part of the Omnicom Group.

A2.2 Document Retention Guidelines

US law criminalises the destruction or alteration of documents with the intent to obstruct a government proceeding. The penalties for this include fines and imprisonment. In the event that a US government investigation (including a voluntary request for information) is likely or has been commenced against the Company or another Omnicom company with respect to which you may have relevant records, you must preserve such records, even if the Company’s general document retention policy could be interpreted as permitting you to destroy them. This obligation is not limited to financial documents and associated records, but includes many other types of records, including those that you may have in your files (both hard copy and e-mail and other electronic files).

If you become aware that the Company (or another Omnicom entity with respect to which you may have relevant records) is the subject of any pending or anticipated US government investigation or litigation, you must cease immediately any alteration, deletion or destruction of records, including electronic records, related to the subject matter of such investigation or litigation. For example, if there is a government investigation into Omnicom's relationship with Client X, and you have e-mails pertaining to that client relationship, and/or copies of contracts with that client, you should take steps so that those records are preserved in case they are requested in connection with the investigation. Please note that this may include investigations of other parties, such as Client X in this example. It is impossible to anticipate the kinds of records that may be implicated in any given US government investigation or litigation, so if you are in doubt about whether you have pertinent records, please ask your manager; or someone within your finance team; or call the Office of Omnicom's General Counsel at (00 1 212) 415 3353.

If you learn that a government investigation is likely or has commenced but we have not brought it to your attention, please notify your manager immediately.

Employees, contractors, temporary employees or agents who knowingly and wilfully violate this policy will be considered to have violated the Omnicom Code of Business Conduct and will be subject to such penalties and reprimands as are appropriate to the circumstances. If you have any questions or concerns regarding this statement, please ask your manager; or someone within your finance team; or the Office of Omnicom's General Counsel, details of which are available on the Omnicom group website – www.omnicomgroup.com.

A.3 COMPUTER SYSTEM POLICY

A3.1 Introduction

The purpose of this policy is to ensure that all of the Company's users use the Company's IT facilities in an effective, efficient, and ethical manner, and also to avoid the risk of the Company and individual employees facing legal liability as a result of improper use, whether inadvertent or deliberate. Persistent breach of this IT policy and/or misuse of the Company's IT facilities would be a disciplinary infringement and may lead to disciplinary action being taken against you, which may include summary dismissal. Nothing in this policy shall prohibit any of the Company's users from making a protected disclosure (often known as 'whistle-blowing') under applicable law.

The Company's IT resources comprise, without limitation, any computer (including laptops issued for off-site use), server or data network, and any telephone handset, switchboard or voice network provided or supported by the Company, and includes interface with and use of public networks in conjunction with the Company's IT facilities.

Use of the IT facilities includes the use of data/programs stored on the Company's computer systems; data/programs stored on magnetic tape, floppy disk, CD-ROM or other storage media owned and/or maintained by the Company; and any Company data held on home computers.

The e-mail facility and access to the Internet and client intranets provided by the Company are intended to promote effective communication for the Company and its clients on business matters. The Company reserves the right temporarily or permanently to limit, withdraw or restrict use of, or access to, any IT facilities if it believes they are being used in an inappropriate manner.

A3.2 Software

Software may carry viruses which could do great damage to the Company's computer systems. Therefore **all** software used on any of the Company's computers must be approved in advance and in writing by the IT Department. Only staff authorised by the IT Department may load software onto any of the Company's computers, connect any hardware or other equipment to any such computers, or move or change any such computer equipment.

You must not make copies of software unless the copyright owner expressly permits this, or as permitted by law.

You must not use software for which the Company does not own a current user licence.

You must not make 'extra' copies of software (the IT Department retains the only lawful back-up copies of all software used in the business).

The Company has committed itself to obeying the user guidelines accepted in the industry, and the Company's reputation could be damaged if it were found to have infringed those guidelines.

If you find you have unlicensed software on a machine for which you are responsible, please contact the IT Department to ensure that it is removed properly. This applies equally to software which you never use. If you are unsure if you have a licence for a particular package, please check with the IT Department. Where you are supplied software on a trial basis, you must either delete it at the end of the specified time or purchase a licence. Please contact the IT Department if you are unsure of how to do this.

If you have a genuine need for a particular software package, please ask the IT Department.

A3.3 System integrity

It is the responsibility of each user to take all reasonable precautions to safeguard the security of the computer and the information contained upon it. This includes protecting it from physical hazards; not allowing unauthorised users access to the machine; and only using approved software.

Our business is vulnerable to computer viruses and Trojan horses. Trojan horses are programs which contain unauthorised instructions included by the programmer for malicious purposes; whilst the program performs the action expected by the user, it also has unseen effects.

An anti-virus software package is installed on each PC/the network and you should run this package to check removable media (such as floppy disks, CDs or USB memory sticks or pen drives) before you use them. If you are unsure of how to do this, please contact the IT Department. However, you should not rely on this software to protect your computer. The other precautions outlined in this policy statement offer maximum protection and you are therefore required to follow these to ensure the system is protected.

You must not use personal memory sticks or portable music players or other ‘mass storage’ devices for the copying of data unless this is authorised in advance and in writing by the IT Department. This is particularly true of such devices given to you by sources outside the Company.

You must not use Company IT systems to create, store, share or distribute data (for example music files, movies etc) that are not for business purposes, unless you receive approval in writing from the IT Department. The IT Department reserves the right to delete such data without warning.

A3.4 Passwords and security

You are responsible for the security of your terminal, PC or laptop and for protecting any information or other data used and/or stored on your terminal, PC or laptop.

You must not make copies of system configuration files for your own unauthorised personal use or to provide to other people/users for unauthorised uses.

You must not allow your PC/terminal to be used by an unauthorised person.

To ensure security for the system, you must keep your passwords confidential and change them regularly. You must not disclose them to anyone, even to IT staff.

When leaving your PC/terminal unattended or on leaving the office, you must log off the system to prevent unauthorised users using your terminal in your absence.

A3.5 Laptops and other portable computers

You are responsible for your portable computer if you use one and must follow the correct procedures. Here are some important ‘dos and don’ts’.

(a) Do not disclose dial-up or dial-back modem phone numbers to anyone.

(b) Do not disclose password to access the Company's IT facilities remotely to anyone, for any reason.

(c) Do not use login scripts which contain passwords or other information of use to hackers.

(d) Do not leave portable computers unattended.

(e) Store portable computers in secure cabinets when not in use.

(f) Be vigilant with your portable computer in public places, as theft is common.

(g) Do not display sensitive information in a public place where the screen could be overlooked.

(h) Do not hold sensitive information on the hard disk.

(i) Do not keep mass storage devices (e.g. memory sticks) containing sensitive information with the computer.

(j) Use a carrying case to reduce the risk of accidental damage.

(k) Ensure that back-ups are made.

(l) Do not lend the portable computer to anyone - even other employees of the Company - without prior approval from the IT Department.

A3.6 Unauthorised access

To protect the Company's computer systems and records and to preserve confidentiality, access to the Company's IT facilities is controlled.

Do not access any part of the IT facilities for which you do not have authorisation.

Do not use - on or in connection with any part of the Company's IT facilities - programs, utilities and/or any other device designed to:

(a) circumvent security measures,

(b) determine or identify passwords, or

(c) breach conditional access systems,

whether they belong to the Company or to third parties.

Such use would be treated as a serious disciplinary matter which, depending on the severity of the case, might lead to your dismissal from the Company.

A3.7 E-mail policy

The e-mail system is the Company's property and the Company reserves the right to monitor and to access any messages in the system.

Do not send messages that are abusive, discriminatory (on the grounds of race, sex, disability, sexual orientation, religious belief, or age), or defamatory, and please bear the following in mind.

(a) You should treat e-mails with the same caution as with any written medium.

(b) Improper statements can give rise to legal action against you and/or the Company.

(c) Advice given by e-mail may be relied upon and contracts may be created.

(d) The mere deletion of a message or file may not fully eliminate it from the system - it may be traced and retrieved at a later date.

(e) E-mail messages, however confidential or damaging, may be disclosed in court proceedings if relevant to the issues.

(f) E-mail messages sent externally may be accessed by others. Therefore it is advisable to check with the client or third party whether they are happy to receive confidential information via email.

(g) You should make hard copies of e-mails that relate to client matters or otherwise need to be retained as a permanent record, as data cannot necessarily be retrieved from back up.

(h) Due to factors outside the Company’s control, the recipient may not receive an e-mail message for several hours.

(i) It is advisable to obtain confirmation of receipt of important messages by requesting faxed or telephone confirmation, or by using the e-mail return receipt facility.

(j) Do not import file attachments or messages from unknown correspondents onto your system without first having them scanned for viruses by the IT Department (please note that what looks like an innocuous TXT file can be a disguised virus or Trojan Horse).

Whilst a degree of personal emailing is acceptable, you should respect the primary purpose of the e-mail system and keep personal use to a minimum. Use of the e-mail system for personal messages is subject to the Company's right to monitor the system for its legitimate business purposes, and by choosing to use the Company's e-mail system to send a personal message you consent to the Company monitoring such messages (including where it is sent using a computer or laptop off-site). When sending personal e-mails that may be interpreted as forming part of the Company's opinion, views, policy, etc, please make it clear that the content or the views are not associated in any way with the Company.

The sending of inconsequential messages, forwarding 'chain letters' or unnecessarily copying e-mails causes e-mail congestion and should therefore be avoided. Remember that messages posted to the Company's intranet use much less space on the system than lengthy e-mails sent to large numbers of people. Please note that messages posted to the Company's intranet are 'permanent' (i.e. not subject to automatic deletion) and are accessible by everyone in the Company. Please contact the IT Department if you would like information on how to post items on the intranet.

Do not circulate large attached files (such as games, screensavers and pictures) within the Company, as this can crash the computer system. Delete such attachments immediately from your inbox and from sent mail.

In order to keep the system running efficiently, tidy up your mailbox regularly, deleting unwanted messages and saving attachments.

A3.8 Internet policy

The Company is committed to use of the Internet to give access to information and facilities relevant to the Company's business and the Company's clients and prospects.

However, the networks used for the Internet are not secure and any communications sent by this means could be accessed or modified by unauthorised individuals.

There are also threats from information obtained from the Internet, virus attachments being the most common.

Therefore, we must ensure that suitable controls are in place to prevent security breaches or other negative consequences, and you must follow procedures which minimise the risks of using the Internet, and follow good practice in the Internet sites you visit.

The Company reserves the right to monitor the system for its legitimate business purposes, and by choosing to use the Company's IT facilities, you consent to the Company monitoring all Internet sites you access (including those accessed using a computer or laptop off-site).

Internet activity (including e-mail) is generally grouped into four categories as follows:

(a) Business use: this includes but is not limited to advertising/media industry reports, economic information, business news, etc.

(b) Non-business but acceptable use: this includes but is not limited to news, weather, responsible brief personal use such as travel information and Internet shopping.

(c) Misuse: this includes but is not limited to excessive time, large downloads, games, chat rooms, discussion groups, movies or film clips, music files, advertising personal goods or services, online trading, sending unsolicited e-mail (the practice known as 'spamming') and the introduction of unauthorised software to the system. Internet Mail and Chat are not permitted unless specifically authorised by the Finance Director or the Chief Executive Officer.

(d) Inappropriate use: this includes but is not limited to pornographic or adult-orientated websites or e-mails, discriminatory or gambling websites (except client related) or e-mails, sites promoting violence, and illegal software.

You must not access sites of an obscene, abusive, discriminatory (on the grounds of race, sex, disability, sexual orientation, religious belief, or age) nature.

You must not, other than in the normal course of employment, trade or attempt to trade or conduct any sales activities (including the solicitation of such activities) which financially commit or could be construed legally to bind the Company or solicit the creation, alteration or performance of any legal or contractual obligation without the prior written approval of the Chief Executive Officer.

You may only download and use software, film clips and music if copyright is not infringed and, where necessary, permission has been obtained from the copyright owner. Failure to do so is likely to place the Company in breach of third party copyright. It is your responsibility to ensure that any copyright restrictions are obeyed and that virus protection procedures are followed.

A3.9 Consequences of a Breach of this Policy

Failure to comply with any aspect of this policy without good reason could result in the removal of privileges to use the computer system for personal purposes and/or:

(a) in the case of employees, in disciplinary action being taken (including dismissal); and

(b) in the case of non-employees, termination of the relationship and/or legal action.

The following will be regarded as gross misconduct and may lead to immediate dismissal of employees or, in the case of non-employees, immediate termination of the relationship:

(a) serious breach of our virus policy;

(b) sending an e-mail which may materially damage our reputation or that of any person or organisation with which we deal;

(c) sending an e-mail which constitutes sexual, racial or other harassment or a breach of our harassment and bullying policy;

(d) deliberately using our internet facilities to access, view, download, print or distribute pornographic, indecent, sexually explicit or obscene material or material likely to cause offence.

Please note that there are also a number of criminal offences connected with the misuse of computer systems, and that the Company reserves the right to inform the police if it believes that such an offence may have been committed.

A.4 LAPTOP & MOBILE PHONE POLICY

Where replacement laptops, mobile phone handsets or mobile phone screens are required within 24 months of receiving a laptop or mobile phone handset, you will be charged on the following basis:

A4.1 Laptops

- One replacement due to accidental damage/loss within first 24 months of having the laptop will not be charged on the assumption that replacement is on a like for like basis
- The second replacement within 24 months will be charged to you at 50% of the full replacement cost
- The third replacement within 24 months will be charged to you at 100% of the full replacement cost

A4.2 Mobile Phones

- One replacement due to accidental damage/loss within first 24 months of having the mobile phone will not be charged on the assumption that replacement is on a like for like basis
- The second replacement within 24 months will be charged to you at 75% of the full replacement cost
- The third replacement within 24 months will be charged to you at 100% of the full replacement cost

A4.3 Theft

Exceptions to the above will be made in the case of loss due to theft that is evidenced by a police report or if the device develops a technical fault (i.e. not user misuse).

A4.4 Smartphone Management Platform

By taking a company funded mobile phone handset you are agreeing to have the handset included in any smartphone management platform the company may utilise from time to time.

A4.5 Data

The company will pay for “fair usage” of data to cover access to e-mail and moderate web access. However, if excessive use is evident, especially when roaming abroad, which will inevitably incur high charges, you will be responsible for any excessive additional costs and will cover such costs by way of deduction from salary.

To minimise the possibility of incurring such costs you should spend a few minutes with our IT staff who will train in you in the relevant aspects of public/private Wi-Fi usage.

We offer employees departing the company the opportunity to port their phone number to another service provider account but expect the transition to happen prior to leaving AMV BBDO.

A.5 CLEAR DESK POLICY

A5.1 Introduction

It is the desire of the agency to provide a safe and secure environment where all agency members can freely perform their job responsibilities. The agency is committed to provide our clients with the confidence that their business is being handled appropriately within the designated levels of confidentiality and security.

To meet these objectives, it is the responsibility of every person in the agency to adhere to this policy. With the implementation of a clear desk policy, the following objectives will be satisfied:

(a) Improving our “green footprint” through maintaining the principle “whatever can be electronic should stay electronic”. Print only when necessary.

(b) Improve protection and integrity of the electronic data based on the classification of the material (public, confidential or highly restricted)

(c) All business documents have a lifecycle and should be destroyed by their end-of-life date. This is true for hardcopy and electronic documents. This is a retention schedule that is published by Omnicom.

A5.2 Clear Desk Expectations:

(a) Every employee should strive to have only the materials they are actively working on for the client or the agency in clear view on their desk.

(b) Where practical, scanners should be used to make electronic copies of all hardcopy material provided by the client or on behalf of the client and store the electronic images on the appropriate file server.

(c) All unnecessary Highly Restricted and Confidential hardcopy material must be shredded or put in the secure shredding bins.

(d) All unnecessary Public hardcopy material must be recycled in the bins provided or placed in the secure shredding bins.

(e) Bulletin boards and walls should not have any Highly Restricted or Confidential client material permanently affixed unless being actively worked on.

(f) Laptop computers should be locked at all times using the locks when left unattended.

(g) All computers should have keyboard lock and screen protection enabled when away from their computer or laptop. The inactivity interval should be set to a maximum interval of 15 minutes but the recommendation is 5 minutes. This should be an automated utility, pushed out as a matter of policy.

A5.3 Recycling/Shredding Expectations:

(a) All “public” paper should be recycled

(b) All “confidential” and “highly restricted” material should be either immediately shredded when no longer necessary or placed in the secure ‘bins”. These bins are locked and will be shredded on a regular basis.

A.6 EU-U.S. Privacy Shield: Employee Privacy Policy

A6.1 Introduction

BBDO Worldwide Inc., BBDO USA LLC and its subsidiaries (collectively, "BBDO") respect your concerns about privacy. BBDO participates in the EU-U.S. Privacy Shield framework ("Privacy Shield") issued by the U.S. Department of Commerce. BBDO commits to comply with the Privacy Shield Principles with respect to Employee Personal Data the company receives from the EU in reliance on the Privacy Shield. This Policy describes how BBDO implements the Privacy Shield Principles for Employee Personal Data.

For purposes of this Policy:

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Employee" means any current, former or prospective employee, intern, temporary worker or contractor of BBDO or any of its EU subsidiaries or affiliates, or any related individual whose Personal Data BBDO processes in connection with an employment relationship, who is located in the EU.

"EU" means the European Union and Iceland, Liechtenstein and Norway.

"Personal Data" means any information, including Sensitive Data, that is (i) about an identified or identifiable individual, (ii) received by BBDO in the U.S. from the EU, and (iii) recorded in any form.

"Privacy Shield Principles" means the Principles and Supplemental Principles of the Privacy Shield.

"Processor" means any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of a Controller.

"Sensitive Data" means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

BBDO's Privacy Shield certification, along with additional information about the Privacy Shield, can be found at https://www.privacyshield.gov/.

A6.2 Types of Personal Data BBDO Collects

BBDO collects Personal Data about Employees to carry out and support human resources functions and activities, including: (i) recruiting and hiring job applicants; (ii) managing Employee communications and relations; (iii) providing compensation and benefits; (iv) administering payroll; (v) processing corporate expenses and reimbursements; (vi) managing Employee participation in human resources plans and programs; (vii) carrying out obligations under employment contracts; (viii) managing Employee performance; (ix) conducting training and talent development; (x) facilitating Employee relocations and international assignments; (xi) managing Employee headcount and office allocation; (xii) managing the Employee termination process; (xiii) managing information technology and communications systems, such as the corporate email system and company directory; (xiv) conducting ethics and disciplinary investigations; (xv) administering Employee grievances and claims; (xvi) managing audit and compliance matters; (xvii) complying with applicable legal obligations, including government reporting and specific local law requirements; and (xviii) other general human resources purposes. BBDO also may obtain and process Personal Data about Employees' emergency contacts and other individuals (such as spouse, family members, dependents and beneficiaries) to the extent Employees provide such information to BBDO. BBDO processes this information to comply with its legal obligations and for benefits administration and other internal administrative purposes.

The types of Personal Data BBDO collects in connection with these activities includes:

- name;
- contact information;
- date of birth;
- government-issued identification information, passport or visa information;
- educational history;
- employment and military history;
- legal work eligibility status;
- information about job performance and compensation;
- financial account information; and
- other information Employees may provide.

BBDO's privacy practices regarding the processing of Employee Personal Data comply with the Privacy Shield Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability.

A6.3 Notice

BBDO notifies Employees about its privacy practices, including the purposes for which it collects and uses Personal Data, the types of Personal Data BBDO collects, the types of third parties to which BBDO discloses the Personal Data and the purposes for doing so, the rights and choices Employees have for limiting the use and disclosure of their Personal Data, and how to contact BBDO about its practices concerning Personal Data. Information regarding BBDO's Employee Personal Data practices is contained in this Policy.

Relevant information also may be found in notices pertaining to specific data processing activities.

A6.4 Choice

BBDO generally offers Employees the opportunity to choose whether their Personal Data may be (i) disclosed to third-party Controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Employee. To the extent required by the Privacy Shield Principles, BBDO obtains opt-in consent for certain uses and disclosures of Sensitive Data. Unless BBDO offers Employees an appropriate choice, the company uses Personal Data only for purposes that are materially the same as those indicated in this Policy. To exercise their choices, Employees may contact BBDO as indicated in this Policy. To the extent and for the period necessary to avoid prejudicing the ability of the company in making promotions, appointments, or other similar employment decisions, BBDO is not required to offer notice or choice to Employees.

BBDO shares Employee Personal Data with its affiliates and subsidiaries. BBDO may disclose Employee Personal Data without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. BBDO also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

A6.5 Accountability for Onward Transfer of Personal Data

This Policy describes BBDO's sharing of Personal Data.

Except as permitted or required by applicable law, BBDO provides Employees with an opportunity to opt out of sharing their Personal Data with third-party Controllers. BBDO requires third-party Controllers to whom it discloses Employee Personal Data to contractually agree to (i) only process the Personal Data

for limited and specified purposes consistent with the consent provided by the relevant Employee, (ii) provide the same level of protection for Personal Data as is required by the Privacy Shield Principles, and (iii) notify BBDO and cease processing Personal Data (or take other reasonable and appropriate remedial steps) if the third-party Controller determines that it cannot meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles. BBDO is not required to enter into a contract to transfer Personal Data to certain third-party Controllers for occasional employment-related operational needs of the company, such as booking flights or hotel rooms or handling insurance coverage.

With respect to transfers of Employee Personal Data to third-party Processors, BBDO (i) enters into a contract with each relevant Processor, (ii) transfers Personal Data to each such Processor only for limited and specified purposes, (iii) ascertains that the Processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the Privacy Shield Principles, (iv) takes reasonable and appropriate steps to ensure that the Processor effectively processes the Personal Data in a manner consistent with BBDO's obligations under the Privacy Shield Principles, (v) requires the Processor to notify BBDO if the Processor determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles, (vi) upon notice, including under (v) above, takes reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the Processor, and (vii) provides a summary or representative copy of the relevant privacy provisions of the Processor contract to the Department of Commerce, upon request. BBDO remains liable under the Privacy Shield Principles if the company's third-party Processor onward transfer recipients process the relevant Personal Data in a manner inconsistent with the Privacy Shield Principles, unless BBDO proves that it is not responsible for the event giving rise to the damage.

A6.6 Security

BBDO takes reasonable and appropriate measures to protect Employee Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the Personal Data.

A6.7 Data Integrity and Purpose Limitation

BBDO limits the Employee Personal Data it processes to that which is relevant for the purposes of the particular processing. BBDO does not process Employee Personal Data in ways that are incompatible with the purposes for which the information was collected or subsequently authorized by the relevant Employee. In addition, to the extent necessary for these purposes, BBDO takes reasonable steps to ensure that the Personal Data the company processes is (i) reliable for its intended use, and (ii) accurate, complete and current. In this regard, BBDO relies on its Employees to update and correct Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized by the Employees. Employees may contact BBDO as indicated in this Policy to request that BBDO update or correct relevant Personal Data.

Subject to applicable law, BBDO retains Employee Personal Data in a form that identifies or renders identifiable the relevant Employee only for as long as it serves a purpose that is compatible with the purposes for which the Personal Data was collected or subsequently authorized by the Employee.

A6.8 Access

Employees generally have the right to access their Personal Data. Accordingly, where appropriate, BBDO provides Employees with reasonable access to the Personal Data BBDO maintains about them. BBDO also provides a reasonable opportunity for Employees to correct, amend or delete the information where it is inaccurate or has been processed in violation of the Privacy Shield Principles, as appropriate. BBDO may limit or deny access to Personal Data where the burden or expense of providing access would be disproportionate to the risks to the Employee's privacy in the case in question, or where the rights of persons other than the Employee would be violated.

Employees may request access to their Personal Data by contacting BBDO as indicated in this Policy.

A6.9 Recourse, Enforcement and Liability

BBDO has mechanisms in place designed to help assure compliance with the Privacy Shield Principles. BBDO conducts an annual self-assessment of its Employee Personal Data practices to verify that the attestations and assertions BBDO makes about its Privacy Shield privacy practices are true and that BBDO's privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.

Employees may file a complaint concerning BBDO's processing of their Personal Data. BBDO will take steps to remedy issues arising out of its alleged failure to comply with the Privacy Shield Principles. Employees may contact BBDO as specified below about complaints regarding BBDO's Personal Data practices.

If an Employee's complaint cannot be resolved through BBDO's internal processes, BBDO will cooperate with the panel of EU data protection authorities established pursuant to the Privacy Shield to address relevant Employee complaints and provide Employees with appropriate recourse free of charge. BBDO also is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

A.7 BLOG AND SOCIAL MEDIA GUIDELINES

A7.1 Introduction

BBDO Worldwide Inc. and each of its affiliated agencies support employees blogging and their use of social media as an important part of the way we do business. These Blog and Social Media Policy & Guidelines (the "Guidelines") have been developed to set forth the best practices and guidelines for employees who maintain personal blogs, post on external or internal Company blogs, or for employees and workers who interact with others using social media sites and applications. These Guidelines remain consistent with the contractual obligations already in place for all employees and workers at the Company. These Guidelines should be read in conjunction with the confidentiality obligations in your contract and also all the other policies contained in this Handbook.

A7.2 General Considerations

Confidential Information: As an employee or contractor, you are under an obligation not to reveal any Company or client confidential information. Therefore, you should ensure that you do not disclose anything confidential online, as such disclosure would violate your obligations to your client.

Professional Manner: Be professional, respectful and use good judgment. Avoid posting things you would not be comfortable saying directly to someone and assume your colleagues and clients will be exposed to your content. Also show consideration for individuals' privacy.

Personal Responsibility: Keep in mind that if you choose to go public with your personal opinions, you may offend others, including your co-workers and current or future clients. You also will be held personally responsible for any commentary deemed to be defamatory or libellous, or for posting content that violates a person's intellectual and other property rights. What you post to the internet is at your own risk and other parties can pursue legal action against you personally for postings. You are expressly prohibited from posting anything to the internet that might in any way bring the Company or any member of the Omnicom Group into disrepute. Therefore, use your own best judgment and think before you post.

Fact-Checking/Transparency. Commentary should be fact-checked, criticism backed up with evidence. Check your spelling and grammar. Make sure you have permission to post any copyrighted items (e.g. images) and be careful about posting or linking to items that may contain viruses. Don't alter previous posts without indicating that you have done so.

A7.3 Work-related Activity

Whether you are blogging or using other social media tools for a client as part of your work, or blogging or using other social media tools on behalf of the Company for our own public relations purposes, your postings will be treated the same way as any other communication created for the Company or a client. Therefore, all work-related postings should go through the normal review and approval process prior to being posted online.

Some bloggers work anonymously, using pseudonyms or false screen names. In all communications online for a client or the Company, you must "*use your real name, be clear who you are, and identify for whom you work*".

Wikipedia Policy. When working with Wikipedia on behalf of a client or the Company, it is paramount that you clearly identify yourself as a representative of the client or of the Company. This can mean setting up an account under your or your client's name or simply using either name in your communications with the Wikipedia community. When considering an edit, whether it's on behalf of the Company or a client, you must use the "Discussion" or "Talk" pages to present your case to the community for why an edit should be made. Under no circumstances should you make edits to client, Company or competitor-related pages without first putting it up for discussion among the Wikipedia community.

A7.4 Internal Company Blogs

If participating within the Company blog landscape, you should keep the following in mind:

You should ensure that your blogging activity does not interfere with your work commitments.

No postings should be critical of or damaging to the Company or its clients, including, without limitation, by posting or linking to harassing, pornographic or indecent content. Though we will not actively screen the content of materials prior to their being posted on the blog, and may not actively monitor the content of such blogs on an ongoing basis, we may prohibit, discontinue or block access at any time and without notice.

Information that is confidential to the Company or a client should not be shared on any blog.

We are a global organization and our employees reflect a diverse set of customs, values and points of view. Be yourself, but be sure that you remain respectful of others, even when you disagree with their opinions. Be cognizant of objectionable or inflammatory topics – such as politics and religion. Focus on topics that are business-related.

The best way to contribute content that others will find interesting is to write about what you know. Posts that help you, your co-workers and/or our clients to do their jobs and solve problems; posts that help to improve knowledge or skills; posts that contribute directly or indirectly to the improvement of the Company's products and services; or posts that help to promote Company values, are all valuable, constructive additions to the conversation.

We will own all original content, ideas, artwork and plans submitted by you to the blog, and may use the same for any purpose whatsoever.

You expressly release the Company from any claim based upon your choice to participate in any other Company blog community.

A7.5 Personal Blogging and Social Media Interaction

If you chose to have your own blog or engage in personal social media activity, you should do so outside of employment hours. Keep in mind that your blog and social media activity are public and that

inappropriate conduct may negatively affect the Company, its affiliates, its clients, and your employment. You should also bear in mind that if you do anything outside work which the Company considers is inappropriate given your role or position at work, you may be subject to disciplinary action in accordance with the Company's policy.

Be mindful of when it is appropriate to identify yourself as a Company employee and post your Company contact information.

Be aware of your professional association with the Company in social networks. If you identify yourself as a member of the Company, ensure your content is consistent with how you would represent yourself in the workplace.

Personal blogs and postings should not discuss clients or their competitors.

If you maintain your own blog or other publicly available site, we recommend that you include the following disclaimer: "*The opinions expressed on this site are my own and do not necessarily represent those of my employer*".

Your site may generate media coverage. If so, you should contact Roy Elvove, Director of Corporate Communications at 212-459-5797 if any such media contact relates to the Company or a client.

If you have any questions regarding this policy and its application to any specific situation, please contact Skip McGovern, Senior Counsel at 212-459-6977 or Jeff Sautter, Director of Human Resources at 212-459-5998.

A.8 TELEPHONE POLICY

A8.1 Personal use

Use of the Company's telephone system for personal calls is at the Company's discretion. By choosing to use the Company's phone system to make personal calls you consent to the Company checking the type, duration and the number of calls made.

The Company also reserves the right to claim reimbursement for personal calls made.

A8.2 Voicemail

When you are away from your office, your phone should be diverted to voicemail, and your voicemail message should be kept up-to-date. This ensures that third parties are promptly informed that you are unable to take their call, and of any alternative arrangements you have made.

Details on how to change your voicemail message can be obtained from the IT Department.

A8.3 Mobile phones and other mobile devices

If you have been issued with a mobile phone, a personal digital assistant (PDA), a Blackberry or other such mobile device by the Company, you should observe the following good practice.

Your mobile device contains confidential information. Use any security measures such as the setting of PIN numbers and passwords as are available on the device. When using your device to access the Internet or WAP services, observe the Company's Internet Policy at all times.

Mobile devices are particularly attractive to thieves. Use common sense and in particular do not use the device in the open where you may be vulnerable to having it snatched from you, and keep the device in a deep pocket or zipped portion of a handbag.

Many services available to mobile device users (such as information services, premium information provider's phone lines, chat services, downloadable games and ring tones) are charged to the mobile phone account. Some of these services are useful business tools, but others are clearly entertainment and leisure services, and the Company reserves the right to pass on to you any charges for these services.

A.9 MONITORING OF COMMUNICATIONS

The Company reserves the right to audit, monitor or record any communications component of its IT and/or telephone facilities and systems:

(a) For compliance with the Company's IT, telephone, e-mail or Internet policies;

(b) To establish the existence of facts;

(c) To ascertain or demonstrate standards which are or ought to be achieved (quality control and training);

(d) To prevent, investigate or detect crime and disciplinary infringements;

(e) To investigate or detect unauthorised or illicit use of the IT system;

(f) To secure, or as an inherent part of, effective system operation;

(g) To determine whether communications are relevant to the business or are personal communications.

The Company may monitor any communications at any time and use any type of monitoring it deems reasonable. You will not necessarily be warned in advance of such monitoring. Whilst consideration shall be given to the privacy of certain information about you which might be identified as a result of such monitoring, you should be aware that the Company might have access to such information without your knowledge and consent.

A.10 DATA PROTECTION POLICY

A10.1 Introduction

In the course of our business, we process data for a wide range of purposes including sales and marketing, management, administration and employment. Some of this data relates to individuals such as our staff or those working for our clients and suppliers or to data relating to our client's consumers. This is known as "personal data". The workplace privacy notice on our intranet and our external privacy notice set out more detail about this.

"Processing" of personal data covers anything done in relation to that data. For example, it includes storing it, sending it to someone else and amending or deleting it.

As an employee, it is essential that you are aware of our responsibilities in relation to data protection and that you do what you can to ensure we meet these. As explained below, we are required to comply with a number of data protection principles.

A10.2 Scope of Policy

This policy applies to anyone working for or engaged by us and involved in the processing of personal data in the European Economic Area. This includes all employees, officers, consultants, contractors, freelancers, volunteers, interns, casual workers and agency workers. When we use the terms 'employee', 'employment' or 'engagement', we mean all of these categories of workers.

It applies to all of our offices in the European Economic Area.

A10.3 Management Responsibilities

Management has overall responsibility for data protection, compliance with data protection legislation and ensuring that we have management and other systems in place to meet our responsibilities.

The Executive Management Team is responsible at an operational level for data protection, compliance with data protection legislation and implementing management and other systems to meet our responsibilities. Their contact details are;

Chief Financial Officer- Suzanne Gilson- GilsonS@AMVBBDO.COM

Group Chairman & Group CEO Cilla Snowball- snowballc@amvbbdo.com

A10.4 Data Protection Principles

In brief, as an organisation processing personal data, we must comply with the data protection principles. These state that when we process personal data:

- We must do so fairly, transparently and lawfully;
- We may only process it for specified and lawful purposes;
- It must be relevant for our purposes, accurate and kept for no longer than necessary;
- We must do so in a way that ensures appropriate security and must protect it from unauthorised and unlawful processing and against accidental loss or damage.

- We must ensure that we uphold any rights that individuals may have in relation to their data.

In performing your role and carrying out your responsibilities, you must do your best to ensure that we comply with these principles. It is particularly important that staff do all they can to ensure that data is kept securely and safely and that procedures designed to achieve this are followed.

A10.5 Compliance Requirements

Comply with policies

Along with this policy, you must comply will all policies that we establish relating to data and any guidance we give. This includes the following:

- Omnicom Group Global Acceptable Use Policy
- Omnicom Group Global Security Policy
- Records Retention Schedule
- Omnicom Records Management Policy
- Omnicom Data Breach Policy and Protocol
- Omnicom DPIA Policy and Protocol

At all times, you must also follow all reasonable directions and instructions relating to data security and privacy.

Proper purposes

Only use data processed in connection with your work for the purposes for which we created or obtained it. Do not use it in a different context. For example, if you receive information about a job applicant in relation to a specific job application, you should only use it for those purposes. You must not use it in relation to a different job unless we have made it clear to the applicant that we may hold the information on file and consider it in connection with other jobs.

You must not store sensitive or personally identifiable information on any company laptop, tablet, mobile device or external storage device unless required by your job function.

Data security

Keep data secure. Amongst other things, you must do the following:

- Passwords and logins

  Change your password regularly and keep them sufficiently long and complex. Do not disclose passwords or login details or give passes or key cards to anyone else.

- Lock screens

  Keep your screen locked when you are away from your desk to prevent unauthorised users from accessing data.

- Encryption and password protection

  Ensure that all laptops, memory sticks, phones and other mobile devices are password protected and have encryption. Never take such devices outside our offices without encryption. You must take care of these devices and keep them secure.

- Use of home devices

  The use of home devices in performing your work must be in accordance with our Omnicom Group Global Acceptable Use Policy.

- Sending emails

  If you send an email, make sure that it is addressed to the person to whom you intend to send it.

- Printers

  If you send a document with personal data to print, do not leave it on the printer where others may see it.

The above sets out only a selection of your data protection duties. The full range of your data protection duties are set out in our Omnicom Group Global Security Policy.

Cloud providers

Never upload data to a cloud provider unless you know that we have approved its use.

Transferring data outside the EEA

We must not transfer data outside of the EEA unless appropriate protections are in place. Do not send data to organisations within our group without checking with the HR Director and/or Chief Financial officer.

Disclosure outside the organisation

Think carefully before sending data outside the organisation. Do not disclose it to persons outside unless you know that they are authorised to receive it and have a proper purpose. For example, do not disclose data about colleagues to consumers or external organisations – unless you know it is appropriate. If you are not sure how best to handle data, receive an unusual request from an unusual source or have any other queries about the handling of data, ask the HR Director and/or Chief Financial officer.

Third party service providers

From time to time we are likely to contract with service providers to process data on our behalf (e.g. with a payroll agency, or for cloud services or marketing analytics). If we do, we are required to impose obligations on the processor relating to matters such as confidentiality, security and inspection. If you are responsible for contracting for such services, you will need to consider data protection and should speak to our HR Director and/or Chief Financial officer.

Building data protection into our systems

We are required to take measures with a view to processing data only in so far as necessary for our specific purposes and seeking to minimise the data processed. In particular, when contracting for or implementing new systems we should, if practicable, seek to build in technical and organisational safeguards. If you are involved in commissioning or working on the specification for a new system, you should discuss our approach with our HR Director and/or Chief Financial officer.

Privacy impact assessments

A privacy impact assessment is a tool to identify, consider and, if practicable, reduce privacy risks. Although assessments can be used in many contexts, where there is likely to be a high risk to privacy, we are required to carry out an assessment. If you are involved in a project that may involve such risks, you should discuss our approach with our HR Director and/or Chief Financial officer.

For more information, see our Omnicom DPIA Policy and Protocol.

Data subject rights

Data subjects (individuals in relation to whom we process personal data) have various rights including the right of subject access (to be told of data processed about them), to have inaccurate data corrected and to have processing restricted or data erased. Whether and how these rights apply depend on the circumstances. If you receive a request by an individual exercising a right (or think that they may be doing so), you should tell our HR Director and/or Chief Financial officer.as soon as possible.

A10.6 What to do if things go wrong – Data Breach

If a data breach occurs, it potentially puts individuals' privacy at risk. This is treated seriously both by us and by the statutory regulator who has power to impose large fines.

A data breach occurs where there is destruction, loss, alteration or unauthorised disclosure of or access to personal data which is being held, stored, transmitted or processed in any way. For example, there is a data breach if you lose a laptop or a USB stick or if you send an email to the wrong person by mistake.

If you discover a data breach, you **must** notify our HR Director and the Chief Financial officer in accordance with our Omnicom Data Breach Policy and Protocol immediately – and preferably within one hour. Depending on context, you may then need to provide further information on the circumstances of the breach.

Failure to notify a breach or to provide information as set out above will be treated seriously and disciplinary action may be taken.

No-one feels good if they leave a laptop on a train or if it is snatched from them in the street. Losing the data or exposing it to risk is much more important to us than losing the equipment. Do not delay – report it! As an organisation we may need to notify the data breach to the regulator – and must investigate and notify within a tight timeline: 72 hours.

For more information, see our Omnicom Data Breach Policy and Protocol.

A10.7 Training and Guidance

We will provide training and guidance to staff to ensure that they understand their responsibilities.

A10.8 Enforcement of this policy

You must comply with this policy and do your best to ensure that it is followed in your day-to-day work. Breaches of this policy will be taken seriously. In serious cases, particularly when data is put at risk (e.g. a data breach) non-compliance may result in dismissal.

A10.9 Status of this policy

This policy does not form part of your contract of employment. Although you must comply with the policy, it does not in itself create contractual rights or obligations. We may amend it at any time but will make any amendments available to you. Nothing in this policy is intended to create an employment relationship between us and any non-employee providing services to us.

A.11 DATA BREACH POLICY & PROTOCOL

A11.1 Introduction

If a personal data breach arises (or is suspected), as an organisation we must take swift and coordinated action. The steps to be taken will depend on the circumstances and risks. An assessment must be made. In some cases, there will be no risk to any individual's personal data – and other than identifying and implementing system improvements to avoid a future breach and documenting steps taken, no action need be taken. In other cases, the position and response may be much more serious or less clear.

The protocol in Section **Error! Reference source not found.** below sets out an approach to handling a breach involving personal data. Although what we will do in any particular case will depend on all the circumstances, the protocol sets out a general approach which should be helpful in handling a breach.

If a personal data breach arises, there is the potential for serious damage to the privacy and other rights of individuals affected, to our reputation and for significant fines from the Supervisory Authority. It is therefore vital that if a personal data breach arises, it is handled promptly, properly and with involvement of senior staff.

Although this policy and protocol is focused primarily on personal data breaches affecting an Omnicom group company and the personal information we handle directly, a similar approach should be taken when personal data are being processed on our behalf by a data processor (e.g. payroll agency or cloud service provider) and a data breach affects that data. In that case, both we and our data processor will have responsibilities. In practice, by executing the actions within the scope of this protocol, we will need to collaborate closely with the data processor. Questions identified in this protocol may be asked of the processor.

The protocol at Section **Error! Reference source not found.** below assumes a 7 stage approach:

1. Assessment of what has happened and risks.
2. Containing and mitigating or limiting damage.
3. Notifying the Supervisory Authority (if required).
4. Notifying individuals affected (if required).
5. Other notifications (if required).
6. Avoiding problems in the future.
7. Documenting the breach (in our Data Breach Log).

These stages are likely to overlap and do not need to be followed sequentially.

A11.2 Scope

This policy applies to anyone working for or engaged by us and involved in the processing of personal information of individuals who are in the European Union. This includes all employees, officers, consultants, contractors, freelancers, volunteers, interns, casual workers and agency workers. When we use the terms 'staff' 'employee', 'employment' or 'engagement', we mean all of these categories of workers.

A11.3 What is a Personal Data Breach?

A personal data breach is breach of security, whether confirmed or suspected, which may compromise the confidentiality, integrity or availability of personal data. A personal data breach can be accidental or deliberate.

- A "confidentiality breach" involves the unauthorised or accidental disclosure of, or access to, personal data.
- An "integrity breach" involves the unauthorised or accidental alteration of personal data.
- An "availability breach" involves the unauthorised or accidental loss of access to, or destruction of, personal data.

So a personal data breach is not just about losing personal data. Here are some examples of when personal data breaches may arise:

- Loss or theft of equipment such as laptops, mobile phones and memory sticks (or of the data stored on the equipment) or documents, files, information on any other media.
- Corruption of a database that cannot be replaced from a backup.
- Corruption of a database that cannot be replaced from a backup.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error – for example sending an email containing personal data to the wrong recipient, or unintentionally deleting personal data which has not been backed up.
- A hacking attack.
- Phishing attacks where information is obtained by deception.

A 'personal data breach' necessarily involves personal data and/or sensitive/special category personal data. If you are in doubt as to whether or not a breach involves personal data, you must still report it in the manner set out below.

A11.4 Report the Breach- Duties of all staff

If any member of staff becomes aware of a confirmed or suspected breach involving personal data, they **must** notify his or her line manager the Chief Financial Officer and HR Director immediately and preferably within one hour. Those managers are responsible for promptly notifying the Information Security Officer.

This must be done even if the member of staff is responsible for the breach – for example, by leaving a device on a train. Although we prefer not to lose devices, ensuring that there is no risk to any personal data on the device is much more important than the device itself.

Depending on context, the member of staff may be required to provide further information on the circumstances of the breach.

Personal data is any information relating to an identifiable person who can be directly or indirectly identified, in particular, by reference to an identifier. A personal identifier is not limited to just a name. It can include an identification number, location data or online identifier, depending on the technology and the way information about that person is collected.

Sensitive/special category personal data has a higher risk profile. It includes information revealing a person's racial or ethnic origin, their political opinions, religious or philosophical beliefs, trade union membership, health, sex life or their sexual orientation. Genetic and biometric data are also included. Similarly, information about criminal convictions/offences has a higher risk profile.

A11.5 Responsibilities – The information Security Officer

The Information Security Officer is responsible for managing our response to a data protection breach (confirmed or suspected), for ensuring that there are adequate staff and other resources available to deal with the breach and, if relevant, for ensuring appropriate and timely notifications to the Supervisory Authority and any individuals who may be affected. The Information Security Officer is also responsible for incorporating any 'lessons learnt' and for documenting the breach.

In handling a personal data breach, it is likely that a number of functional specialties will be necessary (e.g. legal, IT, HR, finance, marketing and PR or support from external providers such as IT forensics). Although it is not practicable to identify in advance which specialisms will be relevant, we have established a Standing Response Team of individuals who may, depending on the circumstances, be relevant. Their roles and contact details are set out in **Error! Reference source not found.**.

Depending on the circumstances, the Information Security Officer may decide to form a small Incident Response Team drawn from relevant members of the Standing Response Team and others who may, in the particular circumstance, be relevant.

If the data breach occurred in circumstances in which a data processor was involved, the Incident Response Team is likely to need to collaborate closely with the data processor.

A11.6 The Protocol

1. **Assessment of what has happened and risks**
   An assessment must be made of what has happened and risks. Matters to be addressed may include:
   - What type of personal data is involved? How sensitive is it? What might happen if it was misused (e.g. credit card or bank account details)?
   - What has happened to the personal data?
   - How has the breach arisen? Did it arise when personal data was being processed by a data processor?
   - Who may be affected by the breach? Staff, customers or clients, suppliers?
   - How many individuals are likely to be affected by the breach?
   - What are the risks to individuals? Those risks can come in many forms, including loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation and loss of confidentiality of personal data protected by professional secrecy.
   - If data has been lost or stolen, are there any protections in place such as encryption? Could the data be used to harm individuals affected?
   - What could the data tell a third party about the individual? For example, could it enable someone to build up a profile of an individual that might be used fraudulently (identity theft)?
   - Are there reputational risks to our business?
   - Are we insured?
   - Should the police be told?
   - If relevant, our contract with any data processor concerned should be reviewed. Ensure that it imposes an obligation to assist us in complying with our personal data breach obligations.

2. **Containment and damage limitation**
   At an early stage, consideration should be given as to how to contain the incident and limit damage:
   - Actions to take may include isolating or closing a compromised section of the network, replacing lost data from a backup, finding a lost piece of equipment or simply changing the locks on the front door.
   - If individuals' bank or credit card details have been lost, consider contacting the bank or credit card company for advice on anything they can do to help prevent fraudulent use.
   - If relevant, are there steps that a data processor should take? Is it doing so?

3. **Notification of the Supervisory Authority**
   On becoming aware of a personal data breach (confirmed or suspected) the Information Security Officer will first liaise with the Head of Legal (and/or external legal counsel) to determine whether a notification to the Supervisory Authority is required.

   If it is determined that a notification is required, it is the responsibility of the Information Security Officer to notify the competent Supervisory Authority of a personal data breach.

   Where the breach involves the personal data of individuals in more than one EU Member State and notification is required, we will need to notify our Lead Supervisory Authority – which is the UK Information Commissioner's Office. We may, in any event, decide to report an incident to a Supervisory Authority which is not our Lead Supervisory Authority if, for example, we know that individuals in the other EU Member State are affected by the breach.

   A list of contact details for all EU Supervisory Authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

   We must notify all personal data breaches to the Supervisory Authority unless:
   - The breach is unlikely to result in a risk to individual's personal data, rights or freedoms; and
   - We can demonstrate that there is no likely risk.

   If, for example, we lose a laptop that has effective encryption in place, it is unlikely that we will need to notify the Supervisory Authority. But we should check that, for example, the password had been held securely.

   If practicable, we must notify the Supervisory Authority within 72 hours of becoming aware of the personal data breach. If that deadline is missed, we will need to explain the delay.

   The notification must include:
   - An explanation of the nature of the breach, including, if possible:
     (a) the categories of data subjects and approximate numbers; and
     (b) the categories of personal data records and approximate numbers.
   - Details of the contact person – normally the Information Security Officer.
   - A description of the likely consequences of the personal data breach.
   - A description of measures we have taken or propose to be taken to address the personal data breach, including any damage limitation measures.

   In some cases, it will not be possible to provide all this information within 72 hours. If so, we should provide what information we have promptly and follow up as and when further information is available.

   Whether a personal data breach is notified or not, the Information Security Officer must ensure that our Data Breach Log – which records details of the breach, its effects and our response – is updated (see section 7 below). Our Data Breach Log must be given to the Supervisory Authority on request to enable it to ensure proper compliance.

4. **Notifying affected individuals**
   If required, it is the responsibility of the Information Security Officer to notify affected individuals of a personal data breach. Again, the Information Security Officer must first liaise with the Head of Legal (and/or external legal counsel) to determine whether we are required to communicate the breach to

those individuals affected and, if so, how (i.e. the channel) and what (i.e. the content) to communicate.

If the personal data breach results in a high risk to the privacy or other rights and freedoms of individuals, we must tell the individual affected without delay unless:

- The individual's personal data was encrypted or other measures had been taken to make it unintelligible to an unauthorised person;
- We have been able to take measures after becoming aware of the personal data breach which mean that there is no longer a high risk to the privacy or other rights and freedoms of any individual affected; or
- Notifying individually would involve disproportionate effort and we publish a notice giving the information publicly – for example, in newspapers.

The information given to individuals should include:

- A description of the nature of the personal data breach.
- The name and contact details of the relevant contact person where more information can be obtained.
- A description of the likely consequences of the data breach.
- A description of measures we have taken or propose to be taken to address the personal data breach, including any damage limitation measures. Where appropriate, it might include specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords where their access credentials have been compromised.

Any communication to individuals affected should be easy to understand and not sent with other information such as newsletters.

5. Other notifications

Without affecting the notification obligations set out elsewhere in this protocol, the Information Security Officer should consider and consult with the Head of Legal (and/or external legal counsel) to determine whether to notify any other third parties of a personal data breach. Notifications may be required under law or contract. Relevant third parties may include:

- Data protection supervisory authorities in non-EU jurisdictions.
- The police.
- Other law enforcement agencies.
- Insurance companies.
- Professional bodies.
- Public or regulatory authorities (for example, the London Stock Exchange).
- Financial institutions.
- Trade unions or other employee representatives.

If required, it is the responsibility of the Information Security Officer to notify those other third parties of a personal data breach.

6. Avoiding problems in the future

Having identified the cause of the personal data breach, we must look at what we can do to avoid such problems in the future and, more generally, how we responded to the breach. This process will be led by the Information Security Officer. Matters to consider include:

- Should security policies and operational procedures be reviewed and remediated?
- Are there systemic problems which require remediation action to reduce the likelihood of further incidents?
- Are there weak points in existing security measures such as allocation of passwords or use of portable devices?
- Had the staff involved in the personal data breach received proper training? Are staff typically adequately trained? Do they understand security issues? At what frequency is update training offered or required?

- If relevant, how has a data processor responded? Are its security measures adequate and compliant with the law? If not, are we satisfied that it has taken action to improve achieve compliance? Should we terminate our contract with the data processor?
- Are our policies on handling personal data and any breaches (such as this one) sufficiently clear? Should they be improved?

7. Documenting the personal data breach

Irrespective of whether the Supervisory Authority and/or individuals affected have been notified, it is the responsibility of the Information Security Officer to update our Data Breach Log to record details of the breach. Those details recorded will include the causes, what took place, the personal data affected, the effects and consequences of the breach along with the remedial action taken the end of the incident. It will also document the reasoning for decisions taken in response to the breach. In particular, if a breach is not notified, a justification for that decision needs to be recorded.

Where applicable, copies of any notification to a Supervisory Authority and communication to those individuals affected must be retained with the Data Breach Log.

A11.7 Status of Protocol

This protocol is intended to be useful guidance on responding to personal data breaches.

A11.8 The Standing Response Team:

Role	Contact details
Chief Financial Officer	Suzanne Gilson – Gilsons@amvbbdo.com
HR Director	Kelly Knight- KnightK@amvbbdo.com
IT Director	Ed Marcarian- MarcarianE@AMVGroup.com
Information Security Officer.	Shaun Belders
General Counsel	Helen Cavanagh- Cavanaghh@bbdoemea.com

A.12 DATA PROTECTION IMPACT ASSESSMENT POLICY & PROTOCOL

A12.1 Introduction

Projects involving the use of personal data can inevitably give rise to privacy and data protection issues and concerns. Taking privacy and data protection considerations into account when designing a project can help us minimise the risk of harm, and promote compliance from the start rather than as an afterthought.

Data Protection Impact Assessments (DPIA) are tools designed to help find and fix privacy and data protection problems, not just in the early stages of planning and developing a project, but throughout its lifecycle.

As an organisation, where we plan any major new projects involving the use of personal data, or plan to make significant changes to existing uses, we must consider whether a DPIA is required.

We are legally required to carry out a DPIA where we plan to use personal data in certain specified ways, or where our use is likely to result in a high risk to individuals. We must also think carefully about doing a DPIA for any other use of personal data that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive/highly personal data or vulnerable individuals.

If we use DPIA the outset to design projects, processes, products or systems with privacy and data protection in mind, it can benefit us in important ways which include:

- Identifying potential problems at an early stage, when addressing them will often be simpler and less costly.
- Increasing awareness of privacy and data protection across our organisation.

- Demonstrating compliance with our legal obligations.
- Reducing the likelihood of an initiative impacting negatively on individuals.
- Protecting our organisation from reputational damage which might otherwise occur.
- Avoiding costly regulatory and/or legal action.
- Building trust and engagement with individuals.

Not carrying out a DPIA when required, carrying out a DPIA in an incorrect way, or failing to consult the Supervisory Authority where required, can result in a fine of up to €10 million, or 2% global annual turnover (if higher).

The protocol at section A12.4 below explains when we need to carry out a DPIA, and how to go about it. The approach set out in the protocol has been developed from guidance issued by the UK Information Commissioner's Office, and the Article 29 Working Party.

The DPIA protocol assumes the following 9 stage approach:

1. Identify the need for a DPIA.
2. Describe the processing.
3. Consider consultation.
4. Assess necessity and proportionality.
5. Identify and assess risks.
6. Identify measures to mitigate the risk.
7. Sign off and record outcomes.
8. Integrate outcomes into project plan.
9. Keep the DPIA under review.

The DPIA process must be documented. The template for recoding the process and its results can be obtained.

A12.2 Scope

This policy applies to anyone working for or engaged by a company in the Omnicom Group of companies and involved in the processing of personal data of individuals who are in the European Union. This includes all employees, officers, consultants, contractors, freelancers, volunteers, interns, casual workers and agency workers. When we use the terms 'staff', 'employee', 'employment' or 'engagement', we mean all of these categories of workers.

All staff are expected to be familiar with this policy and protocol, and to assist in any DPIAs we carry out. Where a member of staff considers that a DPIA is required but has not been carried out, they must immediately notify that concern to their line manager. Her/his line manager must in turn promptly seek assurances on the issue from the member of staff responsible for managing the project/changes in question (the 'Project Manager').

The Project Manager has overall responsibility for making sure that a DPIA is considered/carried out on any major new project which uses personal data or which involves making significant changes to existing uses

The Project Manager's responsibilities include:

- Deciding early in the life of a project whether a DPIA is necessary.
- Deciding how to do the DPIA (including whether it should be outsourced).
- Carrying out the DPIA.
- Consulting with, and seeking advice from, all relevant individuals. Those individuals will likely include (as required) our Data Protection Officer ('DPO') (if we have one), our information security staff, any data processors, our legal advisors, any other relevant experts (either internal or external), individuals affected by the proposed processing, and the Supervisory Authority.

- Checking that the DPIA has been done correctly, if necessary with feedback our legal advisors (internal or external).
- Integrating the outcomes of the DPIA back into the planning and development process.
- Documenting all decisions and reasoning related to the DPIA.

A12.3 When is a DPIA Required?

A DPIA must be carried out by the Project Manager where we plan a new project or significant change involving any type of processing of personal data which is "likely to result in a high risk to the rights and freedoms" of individuals. A DPIA should be carried out as early as possible, and in any event before the intended processing starts.

'Rights and freedoms' are not limited to privacy rights. They include freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

The law does not define what is meant by 'high risk', and it is necessary to consider both the likelihood and severity of any potential harm to individuals. So, for example, high risk could result from either a high probability of some harm, or a lower possibility of serious harm.

Some specific types of processing automatically require a DPIA. These types of processing are not always likely to cause harm, but they always require a DPIA because there is a reasonable chance that the processing might be high risk. Other types of processing require consideration as to whether not they are likely to result in high risk.

A12.4 The Protocol

1. Identify the need for a DPIA

In any major project involving the use of personal data, or where there is a significant change to the nature, scope, context or purposes of our processing, the Project Manager must make an assessment of whether a DPIA is required by using the screening checklists below.

The Project Manager must do a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

The Project Manager must consider whether to do a DPIA if we plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.

- Systematic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

As a rule of thumb, if we plan to carry out a combination of two or more of these processing activities, then a DPIA must be carried out (though in some cases a DPIA may be required if only one of these types of processing is planned).

Here are some examples which show how the criteria should be used to assess whether a DPIA is required:

Examples of processing	**Possible relevant criteria**	**DPIA required?**
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	Systematic monitoring Vulnerable data subjects	Yes
The gathering of public social media profiles data to be used by private companies generating profiles for contact directories.	Evaluation or scoring Large scale Matching or combining datasets Highly personal data	
A hospital processing its patients' genetic and health data.	Sensitive personal data Vulnerable data subjects Large scale	
The use of a camera system to monitor driving behaviour on highways. The controller envisages using an intelligent video analysis system to single out cars and automatically recognise license plates.	Systematic monitoring New technology	
An online magazine using a mailing list to send a generic daily digest to its subscribers.	Large scale	Not necessarily

Once the Stage 1 screening exercise has been carried out, the Project Manager will reach one of three conclusions:

1. A DPIA is required, in which case the Project Manager will move on to Stage 2 of the protocol.
2. A DPIA is not required, in which case the Project Manager must carefully document the decision and her/his reasoning.

3. If the Project Manager is not sure whether a DPIA is required, said individual must consult with our Hr Director and/or of Chief Financial officer in the first instance. If we do not have a DPO, the Project Manager must seek advice from our Legal Department or outside legal counsel. In cases where it is not clear whether a DPIA is required, it may nonetheless still be useful to carry one out.

2. Describe the processing

The Project Manager must describe the nature, scope, context and purposes of the processing.

The nature of the processing is what we plan to do with the personal data. It should include:

- How we collect the data.
- How we store the data.
- How we use the data.
- Who has access to the data.
- Who we share the data with.
- Whether we use any processors.
- Retention periods.
- Security measures.
- Whether we are using any new technologies.
- Whether we are using any novel types of processing.
- Which screening criteria have been flagged as likely high risk.

The scope of the processing is what the processing covers. It should include the:

- Nature of the personal data.
- Volume and variety of the personal data.
- Sensitivity of the personal data.
- Extent and frequency of the processing.
- Duration of the processing.
- Number of data subjects involved.
- Geographical area covered.

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. It should include:

- Whether we are using any novel types of processing.
- Which screening criteria have been flagged as likely high risk.
- The scope of the processing is what the processing covers. It should include the:
- Nature of the personal data.
- Volume and variety of the personal data.
- Sensitivity of the personal data.
- Extent and frequency of the processing.
- Duration of the processing.
- Number of data subjects involved.
- Geographical area covered.

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. It should include:

- Our legitimate interests, where relevant.
- The intended outcome for individuals.
- The expected benefits for us or for society as a whole.

3. Consider consultation

The Project Manager should consider consulting with:

- Any individuals (or their representatives) likely to be affected by the proposed project. Where those individuals have not yet been identified, the Project Manager may need to carry out market research, or contact relevant campaign or consumer groups for their views.
- Our data processors to help us understand and document their processing activities, and identify any associated risks.
- Other relevant stakeholders. Internally, this will likely include those responsible for information security. The Project Manager might also need external advice from lawyers, IT experts, sociologists or ethicists.
- Our DPO (if we have one).
- Our Supervisory Authority (see further below).

If the Project Manager decides that it is not appropriate to consult with others, or the Project Manager's DPIA decision is at odds with their views, then the Project Manager will need to record her/his decision with reasons.

4. **Assess necessity and proportionality**

It is the responsibility of the Project Manager to check that the processing is necessary for, and proportionate, to our purposes, and describe how we will ensure data protection compliance.

In particular, matters to be addressed will include:

- Our lawful basis for the processing.
- How we will prevent 'function creep'.
- How we intend to ensure data quality.
- How we intend to ensure data minimisation.
- How we intend to provide privacy information to individuals.
- How we implement and support individuals' rights.
- Measures to ensure our processors comply.
- Safeguards for international transfers.

5. Identify and assess risks

An objective assessment must be made by the Project Manager of the likelihood and severity of any risks to individuals' rights and interests. Those risks might include:

- Inability to exercise rights (including but not limited to privacy rights).
- Inability to access services or opportunities.
- Loss of control over the use of personal data.
- Discrimination.
- Identity theft or fraud.
- Financial loss.
- Reputational damage.
- Physical harm.
- Loss of confidentiality.

- Reidentification of pseudonymised data

An assessment of the security risks must also be carried out.

It might also be appropriate to consider our own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust

6. Identify measures to mitigate the risk

The Project Manager is responsible for identifying measures we can put in place to eliminate or reduce high risks. These might include:

- Deciding not to collect certain types of data.
- Reducing the scope of the processing.
- Reducing retention periods.
- Taking additional technological security measures.
- Training staff to ensure risks are anticipated and managed.
- Anonymising or pseudonymising data where possible.
- Writing internal guidance or processes to avoid risks.
- Adding a human element to review automated decisions.
- Using a different technology.
- Putting clear data sharing agreements into place.
- Making changes to privacy notices.
- Offering individuals the chance to opt out where appropriate.
- Implementing new systems to help individuals to exercise their rights.

7. Sign off and record outcomes

The Project Manager must then record:

- The outcome of the DPIA, including:
    - What additional measures we plan to take.
    - Whether each risk has been eliminated, reduced, or accepted.
    - The overall level of 'residual risk' after taking additional measures.
    - Whether it is necessary to consult the Supervisory Authority (if there is a residual high risk which cannot be mitigated, and which we propose accepting).
- Any difference(s) of opinion, either with our DPO or anyone else consulted at Stage 3, including any individuals affected.

8. Integrate outcomes into project plan

It is the responsibility of the Project Manager to implement the measures identified at Stage 6, and integrate them into the project plan.

9. Keep the DPIA under review

The Project Manager is responsible for keeping the DPIA under review and revisiting it when necessary – particularly where there is a substantial change to the nature, scope, context or purposes of our processing.

A12.5 Status of protocol

This protocol is intended to be useful guidance on DPIAs. It may be amended from time to time.

A.13 RECORDS MANAGEMENT POLICY

A13.1 Objective

This Records Management Policy and the procedures included in this Policy are designed to ensure that:

- the Records (as defined below) of the Company are created, managed and disposed of in accordance with applicable legal and regulatory record-keeping requirements and the Company's business needs; and
- the Company satisfies its legal duty to retain and preserve materials that have been or might be requested in a pending or anticipated legal proceeding, audit or investigation.

Creating, managing and disposing of Records in accordance with this Policy will make relevant information more readily accessible for legitimate business use, avoid the unnecessary retention of duplicate Records and reduce expenses by eliminating the storage of unnecessary and outdated Records.

A13.2 Retention Schedule.

Specific requirements regarding the length of time particular classes of Records must be retained can be found in the attached "Retention Schedule". The Section below entitled "Maintenance of Records" describes what to do on the expiry of the retention period specified on the Retention Schedule.

Please note that certain temporary items need not be retained in accordance with the Retention Schedule. These temporary items are described below in the Section entitled "Maintenance of Records."

The Retention Schedule will be reviewed annually and revised in accordance with changes in legal requirements or business needs. If you become aware of a conflict between a retention period provided in the Retention Schedule and the law, please resolve it by adhering to the law and notify the Office of the General Counsel so that a correction in the Retention Schedule can be made promptly.

For purposes of this Policy, the term "Records" includes information recorded in any medium, including, but not limited to, any hard-copy or electronic writing (including, without limitation, e-mail), fax, voice mail, instant message, drawing, graph, chart, photograph, audio or video recording, computer application or other data compilation that is (i) created, received or maintained by any Covered Person in that person's business capacity, (ii) relates to the Company or its business, and (iii) in the possession, custody or control of the Company or a Covered Person. Please note that Records that are located in your home or at any other offsite location are subject to this Policy and must be handled accordingly. Regardless of any records management requirement in this Policy, Records subject to a legal hold must be retained in accordance with the legal hold notice distributed by the Office of the General Counsel. Please refer to the section below entitled "Legal Hold Policy and Procedures" for additional information.

A13.3 Legal Hold Policy and Procedures.

When the Office of the General Counsel becomes aware that a legal proceeding, audit or investigation is pending or anticipated, it will promptly notify the appropriate persons and direct that any Records pertaining to that proceeding, audit or investigation be labelled for retention until further notice. The notice from the Office of the General Counsel could take the form of an e-mail, a hard copy memo or a combination of these methods.

If you receive such a notice from the Office of the General Counsel or otherwise become aware that the Company is the subject of any pending or anticipated legal proceeding, audit or investigation with respect to which you have pertinent Records, you must preserve those Records by immediately ceasing any alteration, deletion or destruction of such Records – even if under the current Retention Schedule, or otherwise under this Policy, you would be authorised to do so. This obligation is not limited to financial documents and associated Records, but includes many other types of Records, including those that you may have in your files (both hard copy and e-mail and other electronic files). In addition to the Records that you normally retain, you should also retain anything that might be relevant, such as copies, personal or convenience notes, etc. If you are in doubt about whether you have Records that pertain to a given matter, please ask a Records Administrator or call the Office of the General Counsel.

If you learn that a legal proceeding, audit or investigation is anticipated or has been commenced that has not been brought to your attention by the Company, please notify the Office of the General Counsel immediately. Do not resume normal destruction practices on any pertinent records until you have received formal written notification from the office of the general counsel.

In some cases, local law criminalizes the destruction or alteration of Records with the intent to obstruct a proceeding. The penalties for this may include fines and imprisonment. In addition, Covered Persons who fail to preserve a Record subject to a legal hold notice may be subject to a disciplinary action, up to and including termination of employment or services.

A13.4 Records Creation

Corporate records are not just formal documents drawn up by lawyers. Most records are created by people in the ordinary course of business. When you take notes in a meeting, send an invoice to a customer, fill out a form or send an e-mail, you may be creating a Record. Always think before you write or otherwise record something. All Records should, insofar as reasonably possible, be accurate, complete, precise, relevant, timely, appropriate for retention, properly organized and easily understandable.

Never misstate or mislead in a Record. Do not guess or draw legal conclusions unless requested to do so. Keep in mind that the Records you create today may be used as evidence in a legal case at some point in the future so make certain you are always truthful, provide context for any observations that you make and never use abusive, offensive or harassing language.

Be especially careful when writing an electronic communication in any form. Many people think of electronic communications as casual conversation, unlike a report or a formal memorandum, so they do not always carefully consider what they write. But unlike a telephone conversation, electronic communications can last indefinitely. They can be stored on the Company's servers or saved by the recipient(s). Remember that electronic communications that you create while performing your job are the property of the Company – they are not private. Review your electronic communications with these points in mind before you send them.

If either you or the Company would be embarrassed to see an electronic communication on the front page of a newspaper, do not create it.

A13.5 Maintenance of Records

There are two reasons to retain Records in your files: (i) if you are legally required to do so, or (ii) if there is a legitimate business reason for you to do so. When you review the Retention Schedule, you will see that a legal retention period has been provided. All Records necessary for business purposes must be retained for a period of time that will reasonably assure the availability of those Records when needed, but should be retained no longer than necessary unless approved by a Records Administrator.

Never destroy a Record that is required to be retained by client contract or law as it may result in serious consequences for both you and the Company. It is imperative that you take all necessary steps to ensure that Records required to be retained by law or for business purposes are retained and not destroyed.

Please note that certain temporary items are disposable as soon as they are no longer of use to you. These include:

- Copies of Records that you are certain have been retained in their original form;
- Drafts of Records that are now complete;
- Records that are widely available to the public; and
- Notes taken for personal use or convenience.

Correctly index and store your Records in a manner permitting easy access and retrieval. You should only be in possession of or have access to Records pertaining directly to your functions and duties. Final signed agreements and original Records should be retained (either electronically or in hard copy) in the central files of your department in accordance with the Retention Schedule.

If you have any questions about whether to retain an item, do not retain it in your files indefinitely. The key to a successful Records Management Policy at the Company is its consistent application. Ask a Records Administrator whether it is appropriate to retain the item and, if not, promptly dispose of it. If you accidentally dispose of an item that should have been retained, immediately contact a Records Administrator to determine how to proceed.

At the expiration of the retention period specified on the Retention Schedule and after obtaining any necessary approvals, Records (in all forms, including electronic versions and hard copies) should be promptly disposed of by means appropriate to their nature or level of confidentiality, such as by purging, degaussing (the process of decreasing or eliminating a remnant magnetic field so that data stored on magnetic media such as hard drives cannot be recovered), shredding, or otherwise destroying the Records so they are unreadable or undecipherable and cannot be reconstructed.

Remember that if you have received a legal hold notice from the Office of General Counsel as described above in this Policy in the section entitled “Legal Hold Policy and Procedures”, do not destroy any Records or temporary documents pertaining to that notice.

A13.6 Records Integrity.

Records frequently go through many changes before reaching their final form – and sometimes even after that. Drafts are prepared, updates are made and corrections are often required. Compromising the integrity of a Record, however, such as fraudulently “backdating” a document, is a very serious offense. Falsifying information in a Record is a violation of this Policy and the Omnicom Code of Business Conduct. In addition, tampering with a Record to impair its availability for use in an official proceeding may violate the law and be punishable by fines or imprisonment.

If you discover that a Record in final form is incorrect, please correct it in a manner that makes clear why the change was made and the reason for that change. Please check with a Records Administrator for the approved procedure. Never “backdate” or otherwise enter incorrect dates on any Record with the intention of misrepresenting the actual date of creation or execution. If you have questions regarding the correct date to use for a Record, please check with a Records Administrator or the Office of the General Counsel.

A13.7 Records Security.

It is imperative that confidential information is handled properly in accordance with the Company’s policies. Examples of confidential information include:

- Anything marked “confidential” or “proprietary”;
- Any competitively sensitive information;
- New strategic plans;
- New product designs;
- Personnel records;
- Client information;
- Marketing plans;
- Communications plans, such as advertising plans or media purchases; and
- Financial information, such as non-public regulatory filings or growth forecasts.

The preceding list of confidential information is not meant to be exhaustive.

Documents vital to the Company's ongoing operations, including any information that might reveal the Company's proprietary trade secrets, must be identified and appropriately safeguarded. It is your responsibility to maintain the confidentiality, privacy and security of confidential Records – including Records you discard.

It is important to make sure that Records are kept in an appropriate location. Confidential Records should be stored in a locked cabinet or drawer and information stored electronically should be password-protected. Do not write down your password in a location next to your electronic device for easy access. Avoid sending confidential information over the Internet. If you must send confidential information by e-mail, be sure you are sending it to the correct person(s).

When you have been told by a Records Administrator that it is acceptable to destroy information that is confidential, make certain that you continue to protect the information by purging, degaussing, shredding or otherwise destroying the Records so they are unreadable or undecipherable and cannot be reconstructed. Please note that when destroying hard copy personnel records, or other documents containing employee information, you must shred them.

A13.8 Electronic Records

Electronic Records, which include e-mails that constitute Records, should be retained according to this Policy. Please note, however, that it is important to consider carefully whether an e-mail actually constitutes a Record for purposes of this Policy.

Many e-mails do not qualify as Records; and e-mails that are not Records should be promptly deleted. On the other hand, failure to retain e-mails that are Records can have serious consequences and result in the imposition of substantial penalties. If you are not sure what to do with a specific e-mail or other electronic Record, check with a Records Administrator before you click delete or elect to save it indefinitely. E-mails are automatically deleted from the Inbox, Drafts, and Sent Items folders in the Company's e-mail system 90 days after they are received or sent, and from the Deleted Items folder 7 days after they are placed there. E-mails that need to be retained may be saved in the subject matter folder labelled "Retention" and saved for 540 days.

Please note that the creator of an e-mail is responsible for retaining that e-mail. If an e-mail was created by a non-Covered Person and it is a Record that needs to be retained, each Covered Person who receives the e-mail must retain it (unless otherwise directed by the Office of the General Counsel).

A13.9 Records Archive Procedure.

When it is appropriate to move Records to off-site storage, they should be stored in authorized repositories. Please contact a Records Administrator if you do not know which repositories are authorized. Please label Records clearly. Each label must indicate what the Records are, the year they were created, a destruction date, and the Covered Person or Company department responsible for the Records. Keep in mind that another person must be able to understand from your description what specific Records are maintained in archived files.

A13.10 Termination of Employment/Discontinuance of Services

A Covered Person whose employment with the Company is terminated for any reason, or who has ceased to provide services to the Company, shall turn over properly retained Records to his or her supervisor prior to departure, unless otherwise instructed. In addition, the IT department must be notified at least one week prior to departure, if possible, in order to ensure that the submission of such person's electronic devices and any electronic files which must be retained separately proceeds smoothly.

If a Covered Person is terminated without notice and the procedure above cannot be followed, such person's supervisor shall be responsible for ensuring that all Records are handled according to this Policy.

Please contact your Human Resources department for additional information regarding the procedures that should be followed in the event of a termination of employment or services.

A13.11 Training

All Covered Persons are required to undergo training in the implementation of this Policy.

A13.12 Exception

Requests for exceptions to the requirements of this Policy and the specific requirements of the Retention Schedule must be submitted to the Office of the General Counsel.

A13.13 Interpretation and Assistance

The Office of the General Counsel is responsible for interpreting the provisions of this Policy and the Retention Schedule as they may apply to specific situations. Questions regarding this Policy should ordinarily be addressed to a Records Administrator, who will then relay them to the Office of the General Counsel, if appropriate. If a Covered Person is uncomfortable raising such questions with a Records Administrator, they may be addressed directly to the Office of the General Counsel

A.14 WHISTLEBLOWER POLICY AND PROCEDURE

A14.1 Introduction

The Company encourages a free and open culture in its dealings between its directors, employees and all people with whom it engages in business and legal relations. In particular, as part of the Omnicom Group we have certain obligations to set and maintain the highest professional standards.

This policy is designed to provide guidance to all those who work with us who may from time to time feel that they need to raise certain issues relating to our business practices with someone in confidence. There is also the option of contacting Omnicom direct and further details of this are given below.

This policy is not a grievance procedure. If you have a concern about the way you are being treated as an individual at work (as opposed to a concern about malpractice within the workspace) you should follow the grievance procedure instead.

A14.2 Subject Matters for Disclosure

This procedure will apply in cases where you genuinely and in good faith believe that (for example) one of the following is occurring, has occurred or may occur within our business:

(a) A criminal offence.

(b) Failure to comply with any legal or regulatory obligation.

(c) Any violation of our Code of Business Conduct.

(d) A miscarriage of justice.

(e) Violations relating to accounting or auditing policies.

(f) Danger to the health and safety of any individual.

(g) Deliberate concealment of information tending to show any matter falling within any one of the foregoing.

Please note, however, that you will not be protected from the consequences of making such a disclosure if, by doing so, you commit a criminal offence.

A14.3 Procedure for Reporting

If you wish to raise or discuss any issues that might fall into the above categories you should speak to the AMV Group's Chief Executive Officer who will treat the matter in confidence. On occasions, further investigation may be necessary and you may be required to attend a disciplinary or investigative hearing as a witness. Appropriate steps will be taken to ensure so far as is reasonably practicable that your working environment and/or working relationships are not prejudiced by the fact of your disclosure.

If you wish to remain anonymous, you can use one of the indirect methods and contact Omnicom's General Counsel's office in the US to discuss suspected violations. Please call 00 1 212 415 3364, which is the Internal Control Line number for all employees calling from outside the United States. You may also mail to Omnicom Group Inc., 437 Madison Avenue, New York, New York 10022, for the attention of General Counsel. Further information on this subject can be found on www.omnicomgroup.com.

We stress that all reports will be confidential except as necessary to conduct proper investigations. No one will be disciplined or suffer retaliation for reporting suspected violations that are made honestly and in good faith.

A.15 HEALTH & SAFETY POLICY

A15.1 Our Health and Safety Policy Statement

We wish to ensure, as far as reasonably practicable, the health, safety and welfare of our people and any visitors are protected. Our policy statement is can be found on the intranet.

The Facilities Department have overall responsibility for Health and Safety. If you have any queries or suggestions for improving our environment then please contact the Facilities Department in the first instance.

The Company sees its objectives as the provision and maintenance of a safe office, equipment and good welfare facilities relevant to Health and Safety.

To achieve these objectives, we will:

(a) Undertake health and safety audits and risk assessments

(b) Provide information to assist employees with health and safety issues

(c) Investigate all accidents and incidents and ensure that any recommendations, where practicable, are implemented

(d) Nominate and train fire wardens and first aiders.

(e) Carry out regular health and safety meetings to review the policy and ensure the objectives are being met.

It is also the duty of every employee and others who work at the Company to take care of his/her own health and safety at work, to comply with our safety arrangements and not to do anything to compromise the health and safety of others.

A15.2 Visual Display Unit ("VDU") Regulations and Office Risk Assessments

The furniture in the office is designed so that you are able to adjust your workstations and chairs. Please contact [the Facilities Department] for further information.

The Company will fund sight tests as set out by the VDU regulations. Please contact the HR Department before your appointment to obtain details. In the event that you require glasses solely for VDU use, the Company will make a contribution to cost after written recommendation from an optician is received.

A15.3 Accident Prevention

Please help us to minimise the risk of any accidents at work and remember that if there is an accident we have a legal obligation to record and report it. It is essential that we know where our danger spots are in order that we can take action and reduce the risk of accidents in the future. Please report any accident, however trivial, to the Facilities Department.

A15.4 Safety and Mobile Phones

It is a specific offence to use a hand-held phone, or similar device, when driving. There is a financial penalty and the possibility of conviction in court. Drivers still risk prosecution (for failure to have proper control) if they use hands-free phones when driving and hence the Company does not condone anyone communication on their mobile or other similar device whilst they are driving for any reason whatsoever. If a matter is urgent and cannot wait, then we would expect you to stop off and park somewhere safe as soon as possible and make the call from a stationary vehicle. Before starting out on any journey by car, switch your phone (or where applicable the device) off or forward your phone straight to voicemail.

A15.5 Drugs and Alcohol

If you suspect that anyone in your team or a colleague is suffering from any alcohol or drug addiction or dependency please speak (in confidence) to the HR Department as it is a health and safety, as well as a work performance issue. We would hope that we could be supportive and seek professional assistance for that person before the problem gets out of hand or is severely detrimental to the person's heath.

Whilst we would endeavour to help, if the health and safety of others is affected, work performance is below acceptable levels or a person is drunk or under the influence of drugs at work, the Company has the right to take disciplinary action. This may be summary dismissal, if deemed appropriate, after proper investigation has been carried out. Similarly, if drugs are discovered on the Company's premises, a full investigation and disciplinary hearing will take place and the appropriate authorities may be contacted.

A15.6 Stress

The difficulty with stress is that, as individuals, we can tolerate it at different levels until it causes us damage, unhappiness and even illness. You should try to identify your own limits and speak to your manager if you are feeling that your stress levels are too high. As people can mask stress well, you should try to keep your eyes open for signs of stress in others. Being open and communicating that you are stressed is the first step to finding a solution so please raise the issue with your department head or the HR Department if you believe you are affected.

A15.7 Electrical Equipment

If you believe that there are problems with connections, plugs or faulty equipment then please notify [the Facilities Department] immediately. Please do not attempt to amend electrical faults yourself. Please ensure any electrical equipment brought on to the premises for use is checked by the Facilities Department in advance.

A15.8 Hazards

Please report loose carpet tiles, trailing wires and extension leads etc. to the Facilities Department.

A15.9 First Aid

The most important rule of First Aid is never to ignore an injury. If you are unwell please inform your manager or a First Aid representative. It is important that you don't disappear without telling somebody where you are. We need to ensure that we can check on you from time to time in case the situation escalates. Please also ensure that any accident, however minor, is recorded in the accident book, which is held by the Facilities Department. It is your responsibility to ensure you are aware of who your First Aid contacts are for your floor and information can be found on the intranet.

A15.10 Smoking Policy

The building will be smoke-free at all times and in all offices, conference rooms and open plan.

A15.11 Fire Procedures RE

We will ensure that regular testing of our fire safety equipment is carried out and conduct practice fire drills to ensure that we are prepared in the event of a fire. In addition, the property is equipped with fire and smoke detection.

A15.12 Emergency Exit

Fire signs are placed around the building indicating emergency exits. Please make sure you know where your nearest escape route is.

A15.13 Fire Marshalls

A number of our people are trained as Fire Marshalls. An up to date list of these people is maintained, together with their telephone extension number and floor locations. This list is constantly reviewed so you may be asked to undergo training. Please find out who your local Fire Marshall is and follow their instructions if the alarms sound.

A.16 EQUAL OPPORTUNITIES POLICY

A16.1 Our Policy

We are committed to being an equal opportunities employer and oppose all forms of unlawful discrimination including discrimination because of sex, marriage or civil partnership, gender identity, gender reassignment, pregnancy or maternity, sexual orientation, race, (including national origin and nationality), religion or belief, disability and age. These are known as “protected characteristics”. This includes consistent and objective standards in recruitment, selection, appraisal, promotion, transfer, reward, training, personal development and treatment of people prior to, or after, returning from maternity leave.

The Company requires everyone to act in accordance with this policy and to be treated fairly and without discrimination. If you are subject to harassment based on discrimination or victimised because you have taken action to assert your right not to be discriminated against, you should raise this at the earliest opportunity through our Grievance Procedure. You should be aware also that it is not just the Company who may be liable for unlawful discrimination – sometimes those who participate in unlawful discrimination can be found to be personally liable to the victim. For this reason, any instance of discrimination should be reported to the Staff Relations Department.

All Managers are responsible for ensuring that this policy is applied within their own area. You have a personal responsibility to comply with this policy and do your best to ensure that it is adhered to in your day to day work. You must not discriminate or help others to do so in contravention of this policy. Breaches of this policy will be taken seriously and are likely to result in disciplinary action, up to and including dismissal. You may also be personally liable towards anyone you unlawfully discriminate against, and may have to pay compensation on top of any compensation we might be ordered to pay.

A16.2 Recruitment Practice and Equal Opportunities

Our advertisements and publicity material for the Company should never enhance stereotypes. Any requirements or conditions specified for advertised positions should be carefully considered to ensure that they are necessary for that position. Questions at interview will be limited to those which relate to the suitability of the applicant for the job and applicants will be selected on the basis of fair and objective criteria.

When considering a disabled candidate’s suitability for the job,they should be assessed on the assumption that any reasonable adjustments have been made (for example, if someone needs a special keyboard and this is a reasonable adjustment their ability to do the job compared with other candidates should be assessed on the assumption that the keyboard has been provided). If you are unsure about what questions are appropriate then please contact the Staff Relations Department.

A16.3 Pay and Benefits

Equal pay should be paid for work of equal value, unless there is a genuine material factor that accounts for the variation. Benefits should be offered to all employees equally unless there is a good justification for not doing so.

A16.4 Promotion and Training

Employees should have equal opportunities for promotion and training. When general ability and personal qualities are the main requirements for promotion to a post, care should be taken to consider properly candidates with differing career patterns and general experience. There should be no stereotypical assumptions about the ambitions or otherwise of any individual with a protected characteristic.

Training and development should not stop because someone is pregnant or has childcare responsibilities. Nor should it be assumed that such employees are not interested in promotion.

A16.5 Disciplinary, Performance Improvement and Redundancy Procedures

Care should be taken to ensure that those with a protected characteristic are not sanctioned for performance or behaviour that would be condoned or overlooked in another group. For example a person's gender should not be an accountable factor when dealing with a domestic situation. Any individual should be treated with respect and the situation handled sympathetically.

If selection for redundancy becomes necessary, direct and indirect discrimination should not occur in the selection criteria or process. For example, be careful when using absence-related criteria (because these may disadvantage disabled or pregnant workers) and adjustments might need to be made to ensure that such criteria are fair.

A.17 HARASSMENT POLICY AND PROCEDURE

A17.1 Our Policy

The Company is committed to keeping the working environment free from harassment of any kind by fostering an environment where everyone can work in a professional manner and where relationships with each other are based on dignity and respect. Harassment in the workplace is unacceptable and unlawful. We therefore have a procedure for reporting instances of any harassment and for dealing with the individuals concerned in a confidential and professional way.

Bullying and harassment include conduct that has the purpose or effect of creating an intimidating, degrading or offensive environment. This includes inappropriate actions, behaviours, comments or physical contact that cause offence or objection. This can take the form of physical harassment, ranging from unnecessary body contact to assault; verbal harassment such as unwelcome remarks, suggestions, and propositions, offensive jokes (including those by email), gossip, bullying or pestering or can be non-verbal harassment such as the displaying of offensive literature, pictures/posters graffiti, isolation or non-co-operation. Harassment can affect people in a number of ways, often impacting confidence and self-esteem, and can cause stress and anxiety. It may be classed as bullying.

Individuals who are subjected to bullying and harassment related to “protected characteristics” have special protection. The protected characteristics are age, disability, race, religion or belief, sex, sexual orientation, gender identity and gender reassignment. Both we, as employer, and the person carrying out the bullying or harassment can be liable. If you bully or harass colleagues, you may have to pay compensation personally.

We do not tolerate bullying or harassment whether it is related to protected characteristics or not. This applies not only in the work-place but outside work where there is a work connection – for example at a social event. Such behaviour is normally gross misconduct and likely to result in dismissal; in serious cases, it may be a criminal offence.

Bullying or harassment related to protected characteristics has a broad meaning. It is unlawful:

(a) even though it was unintended and the person doing it was unaware that they might cause offence.

For example, you may feel that you know your colleagues and that they will not be offended by a joke about race, religion, gender identity or sexual orientation, but if they (or someone who over-hears) turn out to be offended, you are likely to be guilty of harassment.

For example refusal to accept or acknowledge a person's chosen gender identity or offensive remarks about gender reassignment.

For example offensive remarks about bisexuality and it’s meaning.

(b) even though the person complaining does not have the protected characteristic.

For example, you are likely to be guilty of harassment if you are white and you make racist remarks about Asians, offending other white people. You are also likely to be guilty if you make homophobic remarks about someone who you think is gay but turns out not to be or about someone who you do not believe to be gay but finds the remarks offensive.

(c) if it is based not on the characteristics of a colleague but on someone they associate with.

For example, offensive remarks to a colleague who is white because they has a black partner.

Sometimes conflicts arise between persons with different protected characteristics (for example sexual orientation and religion). We do not expect everyone to be friends but we do require staff and others to treat each other with respect and dignity regardless of privately held views.

If a client or other third party (someone who is not employed by us) subjects you to harassment or bullying, you should tell us. We will do what we reasonably can to prevent it happening again. If you see this happening to a colleague, you should also tell us.

A17.2 Procedure for Reporting

It is important that if you are the recipient of harassing behaviour, you should feel able to come forward. For this reason, our procedure allows for the resolution of genuine complaints to be treated either formally or informally, as appropriate to the circumstances. Please note that the raising of unfounded allegations for any purpose may be viewed as malicious and may be a serious disciplinary offence in itself.

If you feel that you are being harassed then please raise the matter with a member of the HR Department, as per our Grievance Procedure. All reports will be taken seriously and will be dealt with in a fair and reasonable manner, with respect to confidentiality. Reporting harassment can be done informally or formally with the aim of ensuring that the behaviour stops and that the harasser is spoken to about their behaviour. Formal reporting may be more appropriate if the alleged harasser denies that there is a problem, in order that a written record and proper investigation is carried out.

We will ensure that complaints are treated seriously, promptly and with sensitivity in line with our Grievance Procedure. In each instance every effort will be made to treat the complaint with complete confidentiality although there may be the need, in some circumstances, to refer to witnesses or to directly involve others. There may be instances where the seriousness of the situation or previous informal action proving ineffective or the Company's responsibility to protect you and your associates requires that the Company cannot disregard the information that has come to its attention. In such circumstances, the Company reserves the right to progress the original complaint in line with the formal procedure but commits to making every effort to preserve confidentiality.

On occasions when the informal procedure has proved ineffective, is inappropriate, or serious harassment occurs, then you should bring a formal complaint against the harasser. You should pursue the complaint by reporting the incident(s) to your manager or a member of the HR Department in writing, indicating that you are making a formal complaint.

If an investigation upholds a complaint, action will be taken immediately to stop the harassment and prevent its recurrence. The nature of the penalty imposed upon an employee guilty of harassment will be consistent with those set out in the Company's disciplinary procedure. As part of the Disciplinary Procedure the individual has the right to appeal against any penalty. Similarly, if you have complained of harassment and are not satisfied about the way in which the complaint has been handled, you can ask for it to be reconsidered by another Company director who has not previously been involved. Their decision will be final.

A.18 COMPANY PR/SPOKESPERSON

Do not deal directly with the press or broadcasting world without express permission to do so. All enquiries should be forwarded to the Company's Public Relations Officer or Chief Executive Officer.

PART B – for Company employees only

B.1 PAYMENT OF SALARY

Your salary will be paid directly into your bank or building society account and it is therefore important for you to ensure that the Company has your bank/building society details, P45 and National Insurance number on joining.

Any queries relating to your payslip should be addressed to the Payroll Department, whereas any queries relating to your tax coding should be addressed to the Inspector of Taxes at:

HMRC

West Yorkshire & Craven

Centenary Court

1 St Blaise Wau

Bradford

BD1 4YD

Quote reference: 073 A2475

Tel No: 0300 200 3300

B.2 BENEFITS

Your Contract of Employment states the benefits (if any) to which you are entitled. All benefit schemes are subject to the rules of the relevant schemes, and any limitations imposed by relevant insurers from time to time.

Please be aware that some insurers may require you to attend a medical examination to participate in some of the schemes.

For more information on benefits, please refer to the benefits section on the HR Department Portal.

B.3 ANNUAL LEAVE AND OTHER FORMS OF ABSENCE FROM WORK

B3.1 Entitlement to Annual Leave

All employees are entitled to annual leave as set out in the Contract of Employment.

B3.2 Guidelines for the Booking of Annual Leave

All holidays must be agreed with your manager as early as possible. Managers will normally try to accommodate individual preferences but the needs of the business may have to take precedence, and leave may in some circumstances be refused particularly where inadequate notice is given. Please bear this in mind and, to avoid disappointment, obtain authorisation before booking a holiday.

Any accrued untaken holiday will not be paid or carried over into the following year; therefore it is essential that all accrued holiday days are taken by the end of the calendar year.

B3.3 Special or Compassionate leave

Depending upon the specific circumstances, compassionate or special leave may be granted to you should you experience a serious life event, illness or bereavement in your family, partner or significant other. This may also include supporting a family member or significant person through transitioning.

Compassionate or special leave may normally be granted with pay for an agreed period dependent on your personal involvement. All employees requiring such leave of absence must obtain the prior approval of their department head, and the HR Department should be advised accordingly.

There are separate rules under our Family Friendly Policy, which gives further details of time off for dependents.

B3.4 Jury Service

Should you be asked to attend jury or witness service, please give as much advance notification as you can. In normal circumstances, the Company will agree to leave of absence and you will continue to receive your salary on the basis that any payment/allowances that can be claimed will be claimed and reimbursed in full by you to the Company.

All employees requiring such leave of absence must obtain the prior approval of their department head, and the HR Department should be advised accordingly.

B3.5 Medical and Dental Appointments

If, at any time, you require urgent optical, dental or other medical treatment, the Company will allow reasonable time off subject to approval from your manager. Where possible, such appointments should be arranged outside normal working hours. If this is not possible, appointments should be made at the beginning or end of the working day or during the lunch break.

B3.6 Study Leave

The Company may allow, at its discretion, leave of absence.

B3.7 Unauthorised Absence

Any unauthorised absence is without pay and would be considered a disciplinary offence.

B.4 SICKNESS ABSENCE POLICY

B4.1 Notification

In the event of absence through illness, injury or for any other reason, you must notify your manager as early as possible and no later than one hour after your normal starting time on the first day of absence, giving the reason and expected duration of absence. If you cannot personally contact your manager for any reason, you should arrange for a relative or friend to do so.

The Company has its own Self Certification Form and it is a requirement that you complete this form for all absences through sickness or injury. Please complete the form for every absence (even one day).

Where a period of sickness absence exceeds 7 calendar days, please obtain a Medical Certificate from your GP, which details the reason for the absence and the anticipated duration of the period of sickness absence. This should be sent to the HR Department as soon as possible. In the event of a prolonged period of sickness absence, it is your responsibility to ensure that regular medical certificates are provided, covering the entire period of sickness absence.

You must comply with the notification requirements at all times, as failure to do so may result in a loss of entitlement to sickness payments, or possibly lead to disciplinary action being taken.

B4.2 Payment of Company Sick Pay

Following successful completion of your probationary period, you are entitled to receive Company Sick Pay in any calendar year based on the table below; provided that we are satisfied that the absence is due to a genuine medical reason and subject to the reporting and certification guidelines as set out above.

Continuous Service	**Company Sick Pay**
Year 1 (if joining is after the first working day of the calendar year)	[One twelfth of 4 weeks pay for each completed calendar month of service]
1 calendar year	[4 weeks full pay]
2 calendar years	[6 weeks full pay]
3 or more calendar years	[8 weeks full pay]

The Company will not pay Company Sick Pay during your probationary period.

B4.3 Medical Fitness

If you are absent from work by reason of sickness on a persistent basis or for an extensive period of time or there is frequent intermittent illness, the Company may require you to undertake a medical examination or consultation with an appointed medical practitioner or specialist. This will enable us to establish whether your ability to perform your work to the standard required by the Company has been impaired as a result of the sickness absence. In addition, and in consultation with your GP/specialist, it will allow for a decision to be taken as to what is the best course of action to follow. You will be requested to complete a Medical Consent Form to give permission for your medical condition to be communicated to the Company and allow for a proper review of your case.

B4.4 Prolonged Illness/Long Term Sick Leave

We will endeavour to remain in regular contact with you during any prolonged period of sickness absence to monitor your progress with a view to facilitating your return to work in conjunction with your GP or our company doctor.

Return to work interviews may be carried out and return to work plans drawn up where it is deemed appropriate either to facilitate your return to work after an extensive period or where further support or assistance may be required for any other reason to prevent future periods of absence or enhance performance.

B4.5 Illness during Annual Leave

If a period of illness certified by a valid doctor's certificate runs into previously booked annual leave, you may with your managers' approval defer the leave until a later date in the holiday year.

B4.6 Monitoring of Absence

Absence may be monitored and reviewed by the HR Department. If the frequency or length of sickness absence is unacceptably high, a medical examination may be sought.

B4.7 Termination of Employment

As the Company wishes to maintain full operational capability, it reserves the right to terminate employment or implement the disciplinary procedure for any employees whose sickness record is unacceptable and this could lead to termination of employment.

B.5 MATERNITY LEAVE

This maternity policy is designed to set out your entitlements and if you have any questions or require any further information, please contact the HR Department.

When you tell us that you are pregnant we can arrange a meeting with you to go through our policy in more detail including an illustration of what payments you can expect to receive.

During your maternity leave we may need to make reasonable contact with you for a number of reasons, such as to discuss arrangements for your return to work. You may also undertake up to ten 'Keeping in Touch Days' during your maternity leave – allowing work under your contract of employment – by agreement with the Company. Please note that if you do come into work for more than 10 days you may lose your entitlement to SMP or maternity leave.

If you are expecting, some of the terminology may be a whole new language to you. As a result we have tried to define some of the key terms to help you.

B5.1 Definition of Key Terms

Statutory Maternity Pay ("**SMP**") is the amount payable if you have been continuously employed by us for 26 weeks as at 15 weeks prior to the expected birth of your child. SMP, less tax and National Insurance Contributions, if applicable, will be paid in line with the normal payroll arrangements. SMP is payable only for complete weeks and the weeks are calculated from the start of your maternity pay period.

Expected Week of Childbirth ("**EWC**") is the week in which the baby is due to be born as certified by your doctor/midwife on a certificate called MATB1.

Qualifying Week ("**QW**") is the 15th week before the EWC and is used to determine whether you qualify for SMP and is used to calculate your earnings during the SMP period.

MATB1 Certificate is the maternity benefit certificate given to you by your doctor or midwife. It states the EWC. This certificate is extremely important for calculating your SMP and leave entitlements. It is important that you give us this certificate as soon as you can so we can confirm your entitlements.

Maternity Pay Period ("**MPP**") is the period during which SMP is payable to an eligible employee. It may start at any time from the 11th week before your expected week. The actual start date of the MMP depends on when you start your maternity leave. Generally SMP runs from Sunday to Saturday it is normal to officially start your leave from a Sunday.

B5.2 Your Rights prior to going on Maternity Leave

B5.2.1 Time Off for Antenatal Care

You are entitled to take reasonable time off during your normal working hours to receive antenatal care. Antenatal care includes appointments with the GP, parentcraft, hospital and clinics. Please let your manager know that you will be absent as far in advance of your appointment as possible. You may be asked to produce your appointment card, or some other confirmation of your appointment so please keep them. We would appreciate it if you would arrange appointments so as to cause minimum disruption to your work.

B5.2.2 Health and Safety for Pregnant Persons

On letting us know you are pregnant, we will arrange for a personal risk assessment to be carried out. If your job is identified as carrying any risks for you or your unborn child, arrangements will be made to relieve you from those risks. If you have any concerns about your health and safety at any time during your pregnancy you should speak to the HR Department and alert your manager immediately.

B5.3 Your Rights to Maternity Leave

You are entitled to 52 weeks maternity leave. This is divided into 26 weeks ordinary maternity leave and 26 weeks additional maternity leave.

B5.4 Planning the start of your Maternity Leave

You can begin your OML at any time from the 11th week before EWC. Not later than the start of the 14th week before the EWC you must tell us:

a) That you are pregnant;

b) When your baby is due (your EWC); and

c) The date when you want to start maternity leave.

To enable us to facilitate the start of your OML, please provide your MATB1 certificate and fill in the necessary form available from the HR Department.

B5.5 Automatic start of Maternity Leave

If it has not already begun, your maternity leave period will begin automatically when the baby is born or, if you are absent from work for a reason wholly or partly related to your pregnancy as at any time in the four weeks before the week in which the baby is due.

You should notify the HR Department as soon as is reasonably practicable that you are absent wholly or partly because of pregnancy, or that you have given birth.

B5.6 Compulsory Maternity Leave

Legally, you must have two weeks' compulsory maternity leave from the date your baby is born, irrespective of when your maternity leave period commenced. If necessary, the OML period will be extended to ensure that you are able to take your full period of compulsory maternity leave.

B5.7 Changing the Start Date of your Leave

Please give 28 days' notice of a change to any start date of maternity leave and we will amend the end dates for your OML and AML as applicable.

B5.8 Maternity Pay

To qualify for SMP, you must:

(a) Have been continuously employed by the Company for at least 26 weeks by the start of the 14th week before EWC, (QW).

(b) Have average weekly earnings in the eight weeks prior to the QW of not less than the National Insurance Contributions Lower Earnings Limit.

(c) Still be pregnant 11 weeks before the start of the EWC, or have given birth by that time.

(d) Give us at least 28 days' notice (or if that is not possible, as much notice as you can) of your intention to take maternity leave.

Remember, you will need to tell us:

(a) You are pregnant by providing the MATB1 Certificate.

(b) The week your baby is expected (EWC).

(c) When you want your maternity leave to start.

B5.9 Rates and Payments of SMP, subject to Qualification

For the first 6 weeks of SMP, you are entitled to receive 90% of your average weekly earnings (the "**higher rate**"). For the remaining 33 weeks after that you are entitled to be paid at a set rate, which is determined by the Government each year.

B5.10 Enhanced Maternity Pay

In addition to SMP the Company offers Enhanced Maternity Pay to eligible employees. Enhanced Maternity Pay will commence at the same time as SMP and is paid in addition to SMP.

In order to qualify for Enhanced Maternity Pay you need to have one year's continuous service by the Qualifying Week i.e. the beginning of the 15th week before the expected week of confinement (EWC).

Qualifying employees will receive the following:

The first 6 weeks salary at 100% pay (including higher rate SMP)

Followed by 12 weeks at 50% pay (including 12 weeks at lower rate SMP)

Followed by 21 weeks at the lower rate SMP

B5.11 Return to Work Bonus

In addition to offering Enhanced Maternity Pay during OML, the Company also operate a return to work bonus. In order to qualify for a return to work bonus, you need to have two year's continuous service by the beginning of the 15th week before the expected week of confinement (EWC)

The first return to work bonus payment is paid when you return from maternity leave. The payments are staggered and would continue to be paid over 6 months bringing the total Maternity pay to 60% of your average salary over 26 weeks or 60% of total time if less than 26 weeks.

If the employee leaves any time during the bonus pay period, further payments cease and earlier bonus payments would be repayable.

SMP will be paid in the same way as normal salary and your payslip will be viewable within Reach. Please check with us that we have your up-to-date contact details on file.

SMP cannot normally start being paid earlier than the 11th week before the week in which the baby is due. However, if the baby is born earlier than that, SMP will start the following week.

B5.12 Maternity Allowance

If you have less than 26 weeks' service by the start of the 14th week before the EWC, you are not eligible for SMP. If you fail to qualify, the HR Department will provide you with a form SMP1 which details the reasons for not paying SMP to you. You may then be eligible to claim maternity allowance from the Department for Work and Pensions through Jobcentre Plus offices on completion of form SMP1. Maternity allowance is not paid through the payroll but directly by the local Jobcentre Plus. .

B5.13 Contractual Rights during Maternity Leave

During the OML period, your contract of employment will continue as normal and you will be bound by (and entitled to) all the terms and conditions of your employment, except those obliging you to come to work and those relating to wages or salary.

Even though you have no right to wages or salary during this period unless you qualify for SMP, you will still be eligible to receive benefits under your contract (such as BUPA). You will also continue to accrue your contractual holiday entitlement as normal.

B5.14 Pension Scheme

If you are member of the Company pension scheme, your employer contributions whilst on OML and any period of paid AML will remain unchanged (subject to Inland Revenue limits). However, your personal contributions can cease or become a percentage of maternity pay (subject to Inland Revenue limits). For the period of unpaid AML, the employer contributions cease. Please speak to the HR Department regarding your personal contributions before commencing maternity leave.

B5.15 Returning to Work After Maternity Leave

B5.15.1 Return date

We will assume that you will return to work after 52 weeks leave. If you intend to return to work before this date you must give us eight weeks' notice of your planned return date (unless agreed otherwise by the Company). If you do not, we reserve the right to delay your return to a date, which will ensure that we have had eight weeks' notice (unless otherwise agreed by the Company) or until the end of the AML period if that is sooner. If you are suffering from an illness, at the end of the maternity leave period then normal sickness absence rules will apply.

If you are entitled to OML, you have the right to return from OML to the job in which you were employed before you absence, on terms and conditions no less favourable than those, which would have applied if you had not been absent.

If you are entitled to AML, you have the right to return from AML to the job in which you were employed before your absence or, if that is not reasonably practicable, to another job which is suitable for you and appropriate for you in the circumstances and renumerated no less favourably than had you been at work.

B5.15.2 Holiday Entitlement

Your holiday allocation will continue to accrue at the rate according to the Working Time Regulations during OML and AML. The HR Dept will calculate the overall allocation for you.

Prior to returning to work any accrued holiday will be added to the end of your leave. There will be no payments made in respect of holiday accrued.

If you decide not to return to work you will not be entitled to receive any payments in respect of accrued holiday, as this money will be used to offset any enhanced maternity pay given to you by the company.

B5.16 Not Returning to Work

If you decide you do not wish to return to work, we would really appreciate it if you could let us know as soon as possible, as it is important for us for planning staffing etc. Please also refer to your notice requirements under your contract.

B.6 ADOPTION LEAVE

This adoption policy is designed to set out your entitlements and if you have any questions or require any further information, please contact the HR Department.

When you tell us that you are adopting we can arrange a meeting with you to go through our policy in more detail including an illustration of what payments you can expect to receive.

During your adoption leave we may need to make reasonable contact with you for a number of reasons, such as to discuss arrangements for your return to work. You may also undertake up to ten 'Keeping in Touch Days' during your adoption leave – allowing work under your contract of employment – by agreement with the Company. Please note that if you do come into work for more than 10 days you may lose your entitlement to SAP or adoption leave.

If you are expecting, some of the terminology may be a whole new language to you. As a result we have tried to define some of the key terms to help you.

B6.1 Definition of Key Terms

Statutory Adoption Pay ("**SMP**") is the amount payable if you have been continuously employed by us for 26 weeks your Matching Week. SAP, less tax and National Insurance Contributions, if applicable, will be paid in line with the normal payroll arrangements. SAP is payable only for complete weeks and the weeks are calculated from the start of your adoption pay period.

Matching Date ("MD") is the date when the adoption agency told you that you have been matched with a child.

Matching Week ("**MW**") The week (Sunday to Saturday) when the adoption agency told you that you have been matched with a child, or the date the child enters the UK or when you want your pay to start (overseas adoptions).

Placed This is when the child starts living with your employee permanently with the aim of being formally adopted in the future. The child may have stayed with them before this date

B6.2 Your Rights to Adoption Leave

You are entitled to 52 weeks adoption leave. This is divided into 26 weeks ordinary adoption leave and 26 weeks additional adoption leave.

B6.3 Planning the start of your Adoption Leave

Your leave can start:

(a) on the date the child starts living with the employee or up to 14 days before the expected placement date (UK adoptions)

(b) when an employee has been matched with a child to be placed with them by a UK adoption agency

(c) when the child arrives in the UK or within 28 days of this date (overseas adoptions)

(d) the day the child's born or the day after (parents in surrogacy arrangements)

You must give you 28 days' notice before you would like to be paid Statutory Adoption Pay, unless the time between the child being matched and placed is less than that.

Within 7 days of being matched with a child, please notify us of the date you would like your leave to start and the 'date of placement' - the expected or actual date the child is placed with you.

B6.4 Changing the Start Date of your Leave

Please give 28 days' notice of a change to any start date of adoption leave and we will amend the end dates for your OAL and AAL as applicable.

B6.5 Adoption Pay

To qualify for SAP, you must:

(a) Have been continuously employed by the Company for at least 26 for at least 26 weeks up to any day in the Matching Week;

(b) Have average weekly earnings in the eight weeks prior to the MW of not less than the National Insurance Contributions Lower Earnings Limit.

(c) Give us at least 28 days' notice (or if that is not possible, as much notice as you can) of your intention to take adoption leave.

(d) Provide Proof of the Adoption

Employees must give you proof of adoption to qualify for Statutory Adoption Pay. Proof is not needed for Statutory Adoption Leave unless you ask for it.

For adoption, the proof must show the:

(a) Your name and address

(b) The name and address of the agency

(c) date the child was matched, for example the matching certificate

(d) expected or actual date of placement, for example a letter from the agency

(e) relevant UK authority's 'official notification' confirming you are allowed to adopt (overseas adoptions only)

(f) date the child arrived in the UK, for example a plane ticket (overseas adoptions only)

B6.6 Rates and Payments of SAP, subject to Qualification

For the first 6 weeks of SAP, you are entitled to receive 90% of your average weekly earnings (the "**higher rate**"). For the remaining 33 weeks after that you are entitled to be paid at a set rate, which is determined by the Government each year.

B6.7 Enhanced Adoption Pay

In addition to SAP the Company offers Enhanced Adoption Pay to eligible employees. Enhanced Adoption Pay will commence at the same time as SAP and is paid in addition to SAP.

In order to qualify for Enhanced Adoption Pay you need to have one year's continuous service by the Matching Week.

Qualifying employees will receive the following:

The first 6 weeks salary at 100% pay (including higher rate SAP)

Followed by 12 weeks at 50% pay (including 12 weeks at lower rate SAP)

Followed by 21 weeks at the lower rate SAP

B6.8 Return to Work Bonus

In addition to offering Enhanced Adoption Pay during OAL, the Company also operate a return to work bonus. In order to qualify for a return to work bonus, you need to have two year's continuous service by the Matching Week.

The first return to work bonus payment is paid when you return from adoption leave. The payments are staggered and would continue to be paid over 6 months bringing the total Adoption pay to 60% of your average salary over 26 weeks or 60% of total time if less than 26 weeks.

If the employee leaves any time during the bonus pay period, further payments cease and earlier bonus payments would be repayable.

SAP will be paid in the same way as normal salary your payslip will be viewable within Reach. Please check with us that we have your up-to-date contact details on file.

B6.9 Contractual Rights during Adoption Leave

During the OAL period, your contract of employment will continue as normal and you will be bound by (and entitled to) all the terms and conditions of your employment, except those obliging you to come to work and those relating to wages or salary.

Even though you have no right to wages or salary during this period unless you qualify for SAP, you will still be eligible to receive benefits under your contract (such as BUPA). You will also continue to accrue your contractual holiday entitlement as normal.

B6.10 Pension Scheme

If you are member of the Company pension scheme, your employer contributions whilst on OAL and any period of paid AAL will remain unchanged (subject to Inland Revenue limits). However, your personal contributions can cease or become a percentage of adoption pay (subject to Inland Revenue limits). For the period of unpaid AAL, the employer contributions cease. Please speak to the HR Department regarding your personal contributions before commencing adoption leave.

B6.11 Returning to Work After Adoption Leave

B6.11.1 Return date

We will assume that you will return to work after 52 weeks leave. If you intend to return to work before this date you must give us eight weeks' notice of your planned return date (unless agreed otherwise by the Company). If you do not, we reserve the right to delay your return to a date, which will ensure that we have had eight weeks notice (unless otherwise agreed by the Company) or until the end of the AAL period if that is sooner. If you are suffering from an illness, at the end of the adoption leave period then normal sickness absence rules will apply.

If you are entitled to OAL, you have the right to return from OAL to the job in which you were employed before you absence, on terms and conditions no less favourable than those, which would have applied if you had not been absent.

If you are entitled to AAL, you have the right to return from AAL to the job in which you were employed before your absence or, if that is not reasonably practicable, to another job which is suitable for you and appropriate for you in the circumstances and renumerated no less favourably than had you been at work.

B6.11.2 Holiday Entitlement

Your holiday allocation will continue to accrue at the rate according to the Working Time Regulations during OAL and AAL. The HR Dept will calculate the overall allocation for you.

Prior to returning to work any accrued holiday will be added to the end of your leave. There will be no payments made in respect of holiday accrued.

If you decide not to return to work you will not be entitled to receive any payments in respect of accrued holiday, as this money will be used to offset any enhanced adoption pay given to you by the company.

B6.12 Not Returning to Work

If you decide you do not wish to return to work, we would really appreciate it if you could let us know as soon as possible, as it is important for us for planning staffing etc. Please also refer to your notice requirements under your contract.

B.7 CO-PARENT LEAVE

B7.1 Ordinary Co-Parent Leave

Co-parents may take 1 or 2 consecutive weeks paid Ordinary Co-Parent Leave (OCL) following the birth of their baby, or the placement date of your adoption. The Company offers Enhanced Co-Parent Pay for all employees. The details of which are outlined below.

If you have less than 26 weeks service by the 15th week before the birth of the baby, or at the Matching Week for adoption, then during the agreed co-parent period the Company's Enhanced Co-Parent Pay is 1 week paid leave (inclusive of SPP), the remainder will be paid at SPP.

If you have more than 26 weeks service by the 15th week before the birth of the baby, or at the matching week for adoption, then the Company's Enhanced Co-Parent Pay is 2 weeks paid leave (inclusive of SPP).

If you have more than 1 year's continuous service by the 15th week before the birth of the baby then the Company's Enhanced Paternity Pay is 4 weeks paid leave (inclusive of SPP).

Statutory Paternity Pay (SPP) is the same as flat rate Statutory Maternity Pay (SMP) or Statutory Adoption Pay (SAL) and levels may vary over time according to statute.

To get this entitlement:

(a) You need to tell us in advance the amount of leave and the relevant dates that you wish to take, giving us at least 28 days notice.

(b) You will be asked to formalise your request via email/note to the Company.

(c) You should take the leave within 56 days of the birth or placement of the child, however if for business reasons this is not possible please discuss this with us.

B.8 SHARED PARENTAL LEAVE

In order to qualify for shared parental leave, employees must meet the criteria for co-parent leave (found in the section above).

Shared parental leave and pay enables someone on maternity leave or adoption leave to commit to ending their leave and pay after at least two weeks' maternity or adoption leave and to share the taken balance remaining from the 50 weeks of leave with the co-parent. Eligible carers may share up to 50 weeks of shared parental leave.

Shared parental leave must be taken in blocks of at least one week. The employee can request to take shared parental leave in one continuous block (in which case the organisation is required to accept the request as long as the employee meets the eligibility and notice requirements), or as a number of separate blocks of leave (in which case the employee needs the company's agreement).

You may be entitled to shared parental leave and/or pay if:

a. you are the parent of the child and expect to share the main responsibility for the child (with the other parent);
b. you have at least 26 weeks' continuous employment by the Qualifying Week or Matching Week and are still employed at the time of birth/placement;
c. you meet the government's current lower earnings limit threshold and the other parent or your partner has worked at least 26 of 66 weeks before the EWC/PD and meets an earnings threshold (broadly, £30 average weekly earnings);
d. the mother or main adopter curtails their maternity leave or adoption leave after at least two weeks' leave; and
e. all necessary notices and declarations are provided.

During shared parental leave, you are entitled to 20 SPLIT days in order to keep in touch during your shared parental leave (please see KIT days for more information).

B.9 FAMILY FRIENDLY POLICIES

B9.1 Parental Leave

'Family Friendly' legislation permits time off to care for your child. Subject to the eligibility criteria outlined below, you are entitled to take up to a maximum of 13 weeks unpaid parental leave per child, or 18 weeks if your child is disabled and in receipt of disability living allowance. You will qualify for parental leave if you:

a) Are a parent of a child under 5 (or 18 if disabled), meaning a person named on the child's birth certificate or a person having or expecting to have parental responsibility for the child under the law.

b) Have been continuously employed by us for one year by the time you wish to take the leave: and

c) Are taking the leave to look after the child or make arrangements for the child's welfare.

You should discuss your particular circumstances with the HR Department. Parental leave is always subject to the agreement of your department head so as to ensure that resources can be appropriately managed.

To take advantage of parental leave you must give us at leave 21 days' notice of the dates when you want leave to start and finish.

If we consider that your absence would unduly disrupt the business, we can postpone your leave for up to 6 months (unless it was requested for the birth, in which case we cannot postpone it). We will give notice of the postponement no later than 7 days after your notice to take leave was given to us. We will state the reason for the postponement and set out new dates of your parental leave (and will consult with you about those dates).

B9.2 Time off for Dependents

We will offer you support where possible to assist with any difficult personal circumstances. You are entitled to reasonable time off [unpaid] for family emergencies or dependents in the following circumstances:

(a) When a dependant falls ill or is injured

(b) When a dependant gives birth

(c) To make longer-term arrangements for a dependant who is ill or injured

(d) When a dependant dies

(e) When there is an incident involving your child at school

(f) When there is a disruption or breakdown in care arrangements for a dependant.

All other circumstances for time off for dependants including any substantial time off will be subject to the discretion of the Company.

If you need to take time off for dependants you must tell us as soon as reasonably practicable the reason for your absence (unless it is not reasonably practicable for you to tell us the reason for your absence until you return to work) and how long you expect to be away from work.

B.10 FLEXIBLE WORKING POLICY

B10.1 Introduction

This policy sets out the Company's flexible working policy. It applies to all employees of the Company who have been employed by us for 26 weeks on the date the application is made.

If you have any questions or need further information, please speak to a member of the HR Department.

B10.2 The changes you can apply for

You can apply for a change to:

(a) the hours you work;

(b) the times when you are required to work; and

(c) where,as between our premises and your home, you are required to work.

B10.3 How to apply for flexible working

To make a valid application for flexible working, your application must:

(a) be dated and in writing;

(b) specify the change applied for and the date when you want this change to be effective;

(c) explain what effect, if any, you think making the change would have on us and how, in your opinion, this effect might be dealt with.

(d) State whether you have made a previous application.

Please give or send your application to a member of the HR Department.

It does not matter in what form your application is made. We will consider a request in any form as long as it contains all the details set out above.

Please give as much detail as possible about the change you have applied for and the effect you think this would have on your job, your colleagues and our business. If you think there may be potential problems, please explain how these might be overcome. If you want to change your working pattern on your return from maternity leave, you can apply while still on leave but you should make your application in good time or we may be unable to make a decision before you are due back.

B10.4 Consideration of your application

Once we have received a valid application, the next step is for us to acknowledge receipt and confirm the date when we received it.

Unless we can agree to the change without further discussion, we will hold a meeting with you within 28 days of receiving your application. The meeting will be arranged for an appropriate time and place that is convenient for you and us. Normally, the meeting will be with your head of department and a member of the HR Department. If your department head is off sick or on leave, we may have to delay the meeting.

You have a right to be accompanied by a colleague or certified trade union representative who works at any premises which form part of the business at the meeting.

At the meeting we will discuss the change you have applied for, consider how it might be accommodated, discuss any effects it might have and consider potential problems. All applications will be viewed sympathetically and considered seriously. However, whether such a request will be granted will depend on the circumstances.

We will give you a written decision on your application within 14 days of the meeting. If we refuse your request, we will explain why. We may refuse your request on one or more of the following business grounds:

(a) Burden of additional costs;

(b) Detrimental effect on ability to meet client demand;

(c) Inability to reorganise work among existing staff;

(d) Detrimental impact on quality;

(e) Detrimental impact on performance;

(f) Insufficiency of work during the periods you want to work; or

(g) Planned structural changes.

We will explain which of these grounds apply and why.

B10.5 Appeals

If we refuse your request, you can appeal within 14 days of the date of the written rejection. We will arrange for an appeal meeting to take place within 14 days after receiving your appeal. You have a right to be accompanied by a colleague at the appeal.

We will advise you of the outcome of your appeal in writing within 14 days. If we do not uphold your appeal, we will explain the grounds for that decision and why they apply.

B10.6 Extensions of time

Any extensions of time within this procedure must be agreed between you and us and confirmed in writing, unless the extension is due to your manager being off sick or on leave when you make your application (see above).

B10.7 Withdrawal of application

You can decide to withdraw your application at any time. We will treat your application as withdrawn if you fail to attend two meetings without reasonable cause or unreasonably refuse to provide us with information we require.

B10.8 Further applications

Whatever the outcome of your application (whether it is agreed, refused or withdrawn), you cannot make a further application under for 12 months (and, if making a further application, you must confirm when any previous application was made). This does not necessarily mean that we will refuse to consider any further flexible working requests. It depends on the circumstances and you should discuss this with a member of the HR Department.

B.11 TRANSITIONING AT WORK POLICY

B11.1 Overview

“Transitioning” involves the steps an individual takes to assume the gender they most identify with, not every transition is the same, so it’s important to bear in mind that individuals may need to undergo hormone therapy, surgery or even need mental health support. Whatever the need, it’s important that we are supportive and understanding of the various stages individuals may be going through and to bear in mind that we need to assess requirements, timescales and support on a case-by-case basis.

Under the Equality Act 2010, the ‘process’ or any ‘part of the process’ of moving away from the gender expression typically associated with the sex assigned at birth, towards an expression that reflects the gender identity, is referred to as “gender reassignment”. This is a ‘protected characteristic’ under the Equality Act 2010, which provides legal safeguards against discrimination, harassment and victimisation, from the moment that a person ‘proposes’ to transition.

We have an inclusive culture, so no matter where you come from, your age, religion, gender identity, sexual orientation, race, or background we will support you throughout your time with us. If for any reason anyone is discriminated against or subjected to treatment that may cause upset or offence whether it be by an employee, client or third party, it will not be tolerated and matters will be dealt with promptly and sensitively and in line with our Discrimination, Bullying & Harassment Policies.

B11.2 Once you’ve made the decision to Transition

In order for us to be able to provide you with the support you need it’s important that you speak to your line manager or HR to let them know you’ve made a decision to transition. Once informed, we will be led by you, so in other words you can tell us as much as you feel is necessary to ensure that we provide you with the time, support and work adjustments that you need.

During the course of your transition there will be key things that you’ll need to discuss to help us ensure that we are able to fully evaluate your individual needs at work and to ensure our records are updated with the right information.

The most important step is deciding who you feel most comfortable being your mentor in the Agency. Whilst we know you have great relationships with your Managers, you may decide you’d prefer to have a mentor in the HR team.

Whoever you decide to share your journey with it’s important that you talk to that person about the expected timing of the various stages of your transition so that we can ensure we manage your workloads accordingly. So, if you need time off for medical appointments or procedures, have any adverse side effects to hormone therapy or anything else, keep us informed so we can ensure you don’t worry about work or pay.

As with any situation, we offer a range of mental health support from Self Space to external psychological support, so if you feel you need access to these facilities to aid you in your transition, do reach out to us and will ensure we set up the appointments you need.

We have gender neutral identity cards, gender neutral toilets and allow staff to identify as they feel best suits them.

B11.3 Agreeing Communication

If you want to discuss the best way to communicate your transition, we can talk through options that are Agency led or Employee led, whatever you decide, we will support you.

B11.4 Time off for Medical Procedures/Appointments

At AMV we don't view "transitioning" as sickness, as such all staff will be entitled to up to 8 weeks paid leave to allow for procedures related to transitioning.

If for any reason, you develop a medical condition, as a result of transitioning, then the Agency's sick leave policy will be applied.

B11.5 Confidentiality

We understand that you may wish to keep details of your transition at various stages confidential. Further an individual's transgender status is protected under the Equality Act 2010 and the Gender Recognition Act 2004. Disclosing a person's transgender status without their permission could also result in criminal charges under the Gender Recognition Act 2004.

B11.6 Guidance for Managers

If you chose to disclose your transition to your manager we will ensure they receive a Transitioning At Work training session to equip them to best support you at work.

B11.7 DICTIONARY OF TERMS

Trans – a term used to describe people whose gender is not the same as, or does not sit comfortably with, the sex they were assigned at birth. Those that identify with being trans may describe themselves using one or more of a wide variety of terms, including (but not limited to) transgender, transsexual, gender-queer, gender-fluid, non-binary, gender-variant, crossdresser, genderless, agender, non-gender, third gender, two-spirit, bi-gender, transman, transwoman, trans masculine, trans feminine and neutrois.

Gender Reassignment – To undergo gender reassignment usually means to undergo some sort of medical procedure, but it can also mean changing names, pronouns, dressing differently and living in their self-identified gender.

Gender Expression – how a person chooses to outwardly express their gender, within the context of societal expectations of gender. A person who does not conform to societal expectations may not, however, identify as trans.

Gender Identity – a person's innate sense of their own gender, whether male, female or something else (see non-binary) which may or may not reflect the sex they were assigned at birth.

Gender Recognition Certificate (GRC) – this enables individuals who transition to be legally recognised in their affirmed gender and to be issued with a new birth certificate. Not all individuals who have transitioned will apply for a GRC.

Gender Dysphoria – used to describe when a person experiences discomfort or distress because there is a mismatch between their sex assigned at birth and their gender identity.

Pronoun – words we use to refer to someone's gender in conversation, for example, 'he' or 'she'. Some people may prefer others to refer to them in gender neutral language and use pronouns such as they/their and ze/zir.

Queer –This term has been more recently used by the LGBT community who don't identify with traditional categories around gender identity and sexual orientation, however, it's important to note that some may view this term as derogatory.

Transsexual – this was used in the past as a more medical term to refer to someone who transitioned to the opposite gender to the one assigned at birth. This term is still used by some although many people prefer the term trans or transgender.

Cisgender or cis – someone whose gender identity is the same as the sex they were assigned at birth.

Non-binary – a term for a person who does not identify as only male or only female or who may identify as both.

Intersex – a term used to describe a person who may have the biological attributes of both sexes or whose biological attributes do not fit with societal assumptions about what constitutes male or female. Intersex people may identify as male, female or non-binary.

B.12 DISCIPLINARY POLICY AND PROCEDURE

B12.1 Introduction

We require high standards of conduct and performance from all our staff. This procedure is designed to ensure that all staff are dealt with fairly and consistently if a concern arises over conduct or performance.

Although many concerns about conduct and performance can be handled informally, there will be occasions when this has not worked or informal discussions are not appropriate. In these circumstances, we will normally use this procedure.

When using this procedure, our approach may vary. For example, training and review periods are more likely to be appropriate where the concerns are performance-based as opposed to conduct-based.

B12.2 Overview

If there are concerns about your conduct or performance which we decide to raise under this procedure the key elements of the procedure are that:

We will set out the concerns about your conduct or performance in writing.

We will organise a meeting (which, under this procedure, is called a hearing) to discuss the concerns and listen to your response.

If we decide a concern is justified, we will explain the action we have decided to take.

You may appeal against any action we take.

B12.3 Suspension

If there are concerns about your conduct or performance and we decide to carry out an investigation or hold a hearing under this procedure, we may suspend you. We will only do this if we think it appropriate in the circumstances, for example, where the concern relates to misconduct of a serious nature. Suspension does not imply we believe a concern is justified and is not disciplinary action under this procedure.

B12.4 Investigation

We will look into concerns about your conduct or performance carefully. What is involved will depend very much on the circumstances.

If there are concerns about your conduct, in some cases it will be clear straightaway that holding a hearing under this procedure is appropriate. In other cases preliminary investigation may be necessary before deciding whether to hold a hearing. A preliminary investigation may include interviewing staff and others and reviewing documents. You may be interviewed during such an investigation (but not necessarily).

If there are concerns about your performance, it is less likely that an investigation will be appropriate in advance of a hearing under this procedure.

No decision about whether a hearing should be held will be made until the end of the investigation. In less serious cases of misconduct or in performance matters, the same manager may perform the role of investigator and decision-maker but in serious cases of misconduct we would normally aim to keep these two roles separate.

B12.5 Notification of hearing

Before holding a hearing, we will set out our concerns in writing. If statements have been taken from staff or others, or if there are important documents, we will normally give you copies before the hearing to give you a proper opportunity to respond.

If we decide to hold a hearing under this procedure, we will give you a reasonable opportunity to consider your response to our concerns before the date of the hearing. In practice, we will try to tell you at least 3 working days before the date of the hearing. There are circumstances in which we might hold a hearing with less than 3 working days notice. For example, we might do this if you agree to us doing so or if it is clear that there is no dispute about whether or not a concern is justified.

You must take all reasonable steps to attend the hearing. If, for any reason, you are not able to attend on the date or at the time fixed, you should tell us at once and explain why. If you cannot attend, having said that you would (for example because you become ill), you should tell us as soon possible.

You may choose to be accompanied at the hearing by one of the Company's employees or contractors, or an appropriately qualified trade union official. If the person you wish to attend the meeting with you is unavailable on the date we propose, you must suggest a reasonable alternative time within five days following the original date of the meeting.

B12.6 The hearing

What happens at a hearing will vary depending on the circumstances, but normally:

(a) the manager conducting the hearing will ensure that you understand the concerns raised;

(b) Witnesses may be asked to attend by the Company if the manager conducting the hearing thinks it appropriate, and you may also call your own witnesses. If witnesses attend, the manager will normally conduct any questioning;

(c) you will be given an opportunity to respond to the concerns raised, for example by referring to any documents or statements or other evidence from witnesses;

(d) you will be given a reasonable opportunity to ask questions, and raise points about any information provided by witnesses.

(e) if you choose to be accompanied, your companion may address us at the meeting and you will be allowed to confer with each other, but they will not be allowed to answer questions on your behalf.

Following the hearing the manager will decide:

(a) what, on balance, they think has happened;

(b) if it is not possible to reach a decision, what further investigation is necessary;

(c) whether or not your conduct or performance is below the level required; and

(d) whether or not to take any action.

We will tell you in writing and give you the reasons. We will also tell you of your right to appeal if you are not satisfied with the decision.

The manager who conducts the hearing will usually be your manager, unless this is inappropriate.

B12.7 Further investigations

If, in the light of what is said at the hearing, the manager conducting the meeting thinks it appropriate to look into matters further before making a decision, the individual will tell you and may adjourn the hearing. The task of looking into matters further may be handed back to the investigator. If the results of further investigations are particularly significant, before deciding whether or not the concerns are justified the manager will normally give you an opportunity to comment on the results of the investigations either at a reconvened hearing or in writing.

B12.8 Action under this procedure

If disciplinary action is taken, it will normally take one of the following forms. Taking of action will normally be progressive, but in appropriate cases one or more of the levels may be omitted or repeated.

(a) First written warning ;

(b) Final written warning;

(c) Dismissal (which may be with or without notice).

Performance and misconduct will normally be treated as separate issues and, unless there is a good reason to do otherwise, a warning for one will not justify a higher of level of warning for the other.

B12.9 Review periods

In addition to taking any disciplinary action, the manager will consider whether or not to have a review period. A review period is likely to be appropriate in cases of poor performance or repetitive misconduct such as lateness. During a review period, targets for improvement may be set. Failure to improve adequately during or by the end of a review period may result in further disciplinary action.

B12.10 Training, support, alternative work and demotion

Alongside disciplinary action, there may be circumstances where training, other support or a change in duties or role is appropriate. These are most likely to be relevant in cases of poor performance.

There may also be circumstances where it is appropriate to transfer or demote you as an alternative disciplinary penalty to dismissal.

B12.11 How long does a warning last?

Once a warning is given, we hope there will be an improvement. Unless the warning sets a shorter or longer period, the expiry periods are:

(a) First written warning [12] months;

(b) Final written warning [18] months.

After warnings have expired, they are not destroyed. They are kept on your personnel file, but will not be used in determining the severity of any subsequent disciplinary penalty. They are kept in case we need to refer to them for other purposes (e.g. if a dispute arises over whether or not you were made aware of the inappropriateness of particular conduct or for legal proceedings).

B12.12 Gross Misconduct

Gross misconduct normally results in immediate dismissal without any notice or payment in lieu of notice. The following are examples of conduct often falling within this category:

(a) Negligence, wilful misconduct or deliberate failure to comply with Company's safety rules, regulations, practices or procedures, assets, third party or other personnel is jeopardised.

(b) Serious breach of any Company, client rules and standards that might bring the Company name into disrepute.

(c) Thefts, fraud, deliberate falsification of records, deceit or other dishonesty

(d) Conviction for a criminal offence, which is likely to affect the reputation or the interests of the Company, its employees or clients.

(e) Any act or omission committed with the result of depriving the Company or its clients of money or goods, which belong to or are due to it.

(f) Unauthorised possession of Company property.

(g) Wilful damage to and/or misuse of Company or client's property or premises, or gross negligence resulting in damage or loss of property to the Company or Client.

(h) Wilful disclosure of any confidential information relating to the Company or its subsidiaries business or its client's business to a third party.

(i) Insubordination, insolence, the refusal to carry out reasonable working instructions or any other act of improper behaviour.

(j) Actual or threatened assault upon any fellow employee, member of their respective family, Client's employee or other third party.

(k) Demanding, accepting or offering financial or other inducements either from/to other employees or any third party.

(l) Incapacity or failure to carry out the work duties assigned.

(m) Serious incapability through being under the influence of alcohol or drugs, or taking or possessing drugs, except as prescribed by a Medical Practitioner.

(n) Non-compliance with Company regulations, refusal or failure to observe any of the terms of the Contract of Employment.

(o) Misleading the Company by giving false information or documents in support of your application.

B12.13 Misconduct generally

The following are examples of conduct which may lead to disciplinary action short of immediate dismissal:

(a) poor time-keeping;

(b) unauthorised absence;

(c) abusive/offensive language;

(d) failure to conduct yourself in the Company's best interests;

(e) breach of any policy or term in your contract of employment.

Serious or repeated cases of conduct such as the above may, however, result in immediate dismissal.

B12.14 Appeals

If you wish to appeal against any disciplinary decision, you must tell the Company's Chief Executive Officer. Appeals must be made without unreasonable delay, which will normally mean no longer than five working days after you were told of the decision.

It would be helpful if you set out in writing:

(a) whether you are appealing against the decision that your conduct or performance is below the level required or against level of disciplinary penalty (or both); and

(b) what your grounds are for an appeal.

Appeals against disciplinary action will normally by heard by a person senior to the manager taking disciplinary action.

B12.15 Appeal hearing

You must take all reasonable steps to attend the hearing. If, for any reason, you are not able to attend on the date or at the time fixed, you should tell us at once and explain why. If you cannot attend, having said that you would (for example because you become ill), you should tell us as soon possible.

As at the first hearing, you may choose to be accompanied at the appeal hearing.

The procedure to be followed at the appeal hearing will be determined by the person hearing the appeal. It may vary according to the nature of the appeal.

Appeal hearings will not normally repeat the factual investigation of any preliminary investigation and disciplinary hearing.

At the end of the hearing, the person hearing the appeal will normally adjourn to consider the decision. they may:

(a) overrule the original decision that the concerns (or some of them) were justified; and/or

(b) decide that no action should be taken; or

(c) reduce the level of action taken; or

(d) increase the level of action taken in which case you will have a further right of appeal against the increase.

You will be told of the decision in writing.

B12.16 Grievances and other matters

There may be circumstances where there is an overlap or connection between matters raised under this procedure and matters raised under the grievance procedure. In such circumstances, priority should normally be given to resolving the disciplinary matter (unless the grievance can be resolved quickly). In the interests of fairness, we may need to modify this procedure or the grievance procedure.

B.13 GRIEVANCE PROCEDURE

B13.1 Introduction

The Company does its best to make sure that our people have no reason to complain. However, it is inevitable that problems will arise from time to time. This procedure is designed to help us resolve any grievances raised by our employees.

If you are dissatisfied with any aspect of your employment, it is often best to try to resolve the matter informally by discussing it with your immediate manager. If this is not appropriate, you can discuss it with your head of department or a member of the HR Department.

B13.2 Statement of Grievance

You should set out your grievance in writing and give it to a member of the HR Department.

B13.3 Meeting

We will then invite you to attend a meeting to discuss the matter. The meeting will take place once we have had a reasonable opportunity to consider your grievance, which will normally be within 14 days of receiving your grievance.

You must take all reasonable steps to attend the meeting.

You may choose to be accompanied at that meeting by one of the Company's employees or contractors, or an appropriately qualified trade union official. If the person you wish to attend the meeting with you is unavailable on the date we propose, you must suggest a reasonable alternative time within five days following the original date of the meeting.

During the meeting, we will discuss your grievance, and both of us will have an opportunity to explain our views. If you choose to be accompanied, your companion may address us at the meeting and you will be allowed to confer with each other, but they will not be allowed to answer questions on your behalf.

After the meeting, we will write and tell you our decision.

B13.4 Appeal

If you wish, you may appeal against our decision. You should direct any appeal to the Company's Chief Executive Officer. Appeals must be made without unreasonable delay, which will normally mean no longer than five working days after you were told of the decision.

When appealing, it would be helpful if you would set out in writing what aspects of the decision you are challenging and why.

We will then organise a meeting to discuss your appeal. Appeals will normally be heard by a person senior to the manager who conducted the initial meeting.

You must take all reasonable steps to attend the meeting. As at the first meeting, you may choose to be accompanied.

After the appeal meeting, we will tell you our final decision.

B13.5 Additional Steps

We may take some additional steps where we think this will be helpful, such as holding more than one meeting with you, or adjourning a meeting so that we can carry out further investigations.

B13.6 After termination of employment

This procedure also applies where you have already left our employment. However, if we both agree, we can use a shorter procedure after you have left employment. Under the shorter procedure, you should send your written grievance to the Company's Chief Executive Officer, and we will send you our response in writing.

B13.7 Grievances about harassment or bullying

If your grievance concerns harassment or bullying, you can follow either this procedure, or the procedure set out in the Harassment Policy.

B.14 PERFORMANCE IMPROVEMENT PROCEDURES

We hope we do not have cause to raise any serious performance or capability issues with you. If we do, our Performance Improvement Policy is designed so that issues or concerns may be dealt with in a fair and consistent manner.

B14.1 Policy Principles

The Company aims to ensure that the following principles are applied when dealing with any performance concerns:

You will have an opportunity to answer criticisms of your performance and will be given an explanation for any action taken and the consequences of it at a formal meeting.

Where you need training, support or clarification of your job and its duties in order for you to attain the necessary standards, the Company will do what is reasonable to give such training, support or clarification.

You have the right to be accompanied by a work colleague or union representative at any meetings that may result in the imposition of a warning or dismissal. In instances where your colleague cannot attend on the date proposed you can offer an alternative time and date so long as it is reasonable and falls before the end of the period of five working days beginning with the first working day after the day proposed. The work colleague has a right to address the hearing but no right to answer questions on your behalf.

You have the right of appeal against any level of warning or dismissal imposed as a result of unsatisfactory performance. This should be done by appealing to the HR Department without unreasonable delay, which will normally mean within 5 working days of the written response. Please do so in writing stating the reasons why you believe a further review is necessary.

This procedure may be varied at any stage if it is considered that the situation is serious enough to justify such action.

B14.2 The Performance Improvement Process

We consider all negative feedback constitutes an informal warning since it highlights aspects of your performance that need to be addressed. We believe minor issues should be dealt with informally via manager feedback and/or the appraisal process.

The following is required for more serious or continued concerns about performance:

B14.2.1 **Stage 1: FIRST Formal Warning**

You will be given a warning in writing which will explain the standards that are expected, the shortfalls in your performance and specify a reasonable time within which you must improve. Your performance will be monitored throughout that period (normally by your manager) and a review meeting will be held at the end to consider whether you:

(a) should be given a further period within which to improve (e.g. if circumstances outside your control have prevented you from attaining a satisfactory level of performance); or

(b) have attained a satisfactory level of performance; or

(c) should receive a further warning (see below).

If you have attained a satisfactory level of performance, the first warning will remain on your personnel file for a further six months but will be disregarded at that point if there are no further concerns about your performance.

B14.2.2 **Stage 2: SECOND Written Warning**

In the event of more serious concerns about your performance, or failure to improve or maintain performance during the existence of a previous warning you will be given a further written warning. Again, this warning will explain the standards that are expected, the shortfalls in your performance and specify a reasonable time within which you must improve.

Your performance will be monitored throughout that period (normally by your manager) and a review meeting will be held at the end to consider whether you:

(a) have attained a satisfactory level of performance; or

(b) should be considered for a more suitable role within the Company

(c) receive a Final Warning

If you have attained a satisfactory level of performance, the warning will remain on your personnel file for a further twelve months but will be disregarded at that point if there are no further concerns about your performance.

B14.2.3 **Stage 3: FINAL Warning**

In the event of more serious concerns about your performance, or failure to improve or maintain performance during the existence of previous warnings, you will be invited to a meeting and given a FINAL WRITTEN warning. This warning will explain the standards that are expected, the shortfalls in your performance and specify a reasonable time within which you must improve (which will not normally exceed one/two months). It will also state that if you are unable to turn the situation around, then termination of employment will be necessary. It will advise of right to appeal.

At a review meeting, it will be considered whether you:

(a) have attained a satisfactory level of performance;

(b) or need to be dismissed

B14.2.4 **Final Stage: Dismissal**

In the event of serious under-performance or a failure to improve or maintain performance after reasonable warning/s under this procedure, dismissal will result. You will not be dismissed until you have had an opportunity to set out your position and explain any mitigating factors.

B14.3 Appeals

You may appeal against a decision under this procedure. Any appeal should be made without unreasonable delay, which will normally mean within 5 working days of the notification of the decision indicating the specific grounds of the appeal. Appeals should be communicated to the HR Department who will advise you of the most appropriate senior manager to re-consider your case.

B14.4 Misconduct

In some circumstances, the Company may consider that your unsatisfactory performance amounts to, or has become, a matter of misconduct. This may arise where it seems that you are deliberately failing to try to improve or you are deliberately failing to co-operate with the Performance Improvement Policy. In these circumstances the Company will normally initiate its disciplinary procedure at a stage, which it considers appropriate in the circumstances.

B.15 LEAVING POLICY AND PROCEDURE

B15.1 Resignation

Resignations should be submitted in writing to your manager, giving your contractual notice, and copied to the HR Department.

The Company will contact you confirming your last day of employment and make arrangements for the return of Company equipment and the issuing of your P45 and final pay.

B15.2 Exit Interviews

It is the Company's policy to conduct exit interviews on a voluntary basis with all leavers. These interviews are intended to help us understand if there is anything you believe the Company could do better.

B15.3 P45 and Final Payment

Payment will be made for holiday earned but not taken for the calendar year in which you leave. No payment will be made for public holidays occurring after your last day of employment e.g. if your last day is the Thursday before Easter you would not be paid for Good Friday or Easter Monday.

Final payment is made on the normal pay date in the month in which you leave. P45's are generally issued around the same time. Final payment will only be released once all Company property in your possession has been returned to the Company and when all timesheets have been completed.

B15.4 References

If in the future you require an employment reference from the Company please contact the HR Department in the first instance. The scope may be limited to factual matters such as position and length of service. All information will be given in good faith and no responsibility can be accepted for any loss or damage which may result from such statements.

B.16 RETIREMENT

The Company does not have a formal retirement age, however, most insured benefits will cease at age 65.

B.17 PERSONAL PROPERTY

You are responsible for the safe keeping of your own personal property when at work. The Company assumes no responsibility for any items lost. Any loss should, however, be reported immediately to [the Facilities Department]. Please note that there is no Company insurance for personal items and you should ensure you have suitable and adequate private insurance in place.

B.15 The Halo Code

Our workplace champions the right of staff to embrace all Afro-hairstyles. We acknowledge that Afro-textured hair is an important part of our Black employees' racial, ethnic, cultural, and religious identities, and requires specific styling for hair health and maintenance.

We celebrate Afro-textured hair worn in all styles including, but not limited to, afros, locs, twists, braids, cornrows, fades, hair straightened through the application of heat or chemicals, weaves, wigs, headscarves, and wraps.

In this workplace, we recognise and celebrate our colleagues' identities. We are a community built on an ethos of equality and respect where hair texture and style have no bearing on an employees ability to succeed.

- Notes:

1. Race-based hair discrimination is illegal under the Equalities Act 2010. Workplaces have the right to enforce a dress code as long as it is fair and does not unduly discriminate against any staff. Policies and practices that prohibit hairstyles which are primarily used to maintain Afro-textured hair can lead to indirect discrimination.
2. The Halo Code focuses on hair textures and styles most commonly associated with the Black community. The term Black has historically been used as a racial and political label. Here, we use it to refer to members of the African diaspora, including those with mixed heritage, who as a result of their ancestry have Afro-textured hair.
3. The Halo Code is a gender neutral policy.
4. In order to embody the sprit of The Halo Code, all staff are encouraged to familiarise themselves with different Afro-textured hairstyles and their cultural significance, and to avoid labelling Afro-textured hair with terms such as messy, unprofessional, or inappropriate.
5. The Halo Code does not prevent workplaces from issuing additional guidance around Afro-texture hair and protective styles if applied consistently across all students and staff, including:

- That head wraps and scarves should reflect other elements of the uniform code such as the school's colours.
- That hair be tied up for health and safety reasons, such as during sports, science labs, or to avoid trip hazards.
- That hair colour is reflective of wider school uniform policy.