Data Protection and Information Security

February 2020

ALFRED H KNIGHT

Securing our Data

Data Protection and Information Security are inextricably linked. All organisations have access to confidential information from their own workforce or those of their client's. This combined policy sets out how AHK manages and protects this data and all other data of a confidential nature

Data Protection

AHK obtains, keeps and uses personal information (also referred to as data) about job applicants, employees, temporary workers, contractors, apprentices, clients and suppliers for a number of specific lawful purposes such as ensuring employees are paid correctly and keeping contact details up to date and accurate.

This part of the policy shall set out how we comply with our data protection obligations and seek to protect personal information relating to our workforce or that of our client's. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our, and our client's, workforce, and how (and when) we delete that information once it is no longer required.

Information Security

AHK is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

Under the current legislation, AHK must use technical and organisational measures to ensure confidential or personal information

is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. AHK must be able to demonstrate robust data compliance measures in our daily activities.

The purpose of this part of the policy is to protect against potential breaches of confidentiality, to ensure all our information assets and IT facilities are protected against damage, loss or misuse and to support AHK's data protection policy (contained in the first part of this document) in ensuring all staff are aware of and comply with UK law, and AHK's procedures for the processing of personal information.

Our aim is to increase awareness and understanding within AHK of the requirements for information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

PART 1 - Data Protection

You must read this policy because it gives important information about:

- the data protection principles with which AHK and its employees must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Scope

This policy applies to the personal information of applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

Staff should refer to AHK's data protection privacy notice (provided to you on joining and available on the intranet) and, where appropriate, to any other relevant policies including in relation to internet, email and communications, monitoring, social media, information security, data retention, which contain further information regarding the protection of personal information in those contexts.

We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data', 'special category data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Data protection principles

AHK will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and we will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Basis for processing personal information

In relation to any processing activity, we will, before the processing starts for the first time and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
  - (a) that the data subject has consented to the processing;
  - (b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - (c) that the processing is necessary for compliance with a legal obligation to which AHK is subject;
  - (d) that the processing is necessary for the purposes of legitimate interests of AHK or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
- keep the LIA under review, and repeat it if circumstances change; and
- include information about our legitimate interests in our relevant privacy notice(s).

Sensitive personal information

AHK may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- we have a lawful basis for doing so, e.g. it is necessary for the performance of the employment contract, to comply with AHK's legal obligations or for the purposes of AHK's legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, e.g.:
  - (a) the data subject has given explicit consent;
  - (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of AHK or the data subject;
  - (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
  - (d) processing relates to personal data which are manifestly made public by the data subject;
  - (e) the processing is necessary for the creation, exercise or defence of legal claims; or
  - (f) the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify the data protection officer of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until:

- the assessment referred to above has taken place; and
- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

AHK will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

AHK's data protection privacy notice sets out the types of sensitive personal information that AHK processes, what it is used for and the lawful basis for the processing.

In relation to sensitive personal information, AHK will comply with the procedures set out in the below paragraphs to make sure that it complies with the data protection principles set out above.

During the recruitment process: the HR department, with guidance from the data protection officer, will ensure that (except where the law permits otherwise):

- during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;
- if sensitive personal information is received, e.g. the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
- any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;
- 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
- we will only ask health questions once an offer of employment has been made.

During employment: the HR department, with guidance from the data protection officer, will process:

- health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;
- sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and
- trade union membership information for the purposes of staff administration and administering 'check off'.

Criminal records information

Criminal records information will be processed in accordance with AHK's Criminal Records Information Policy.

Data protection impact assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where AHK is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer in order that a DPIA can be carried out.

Documentation and records

We will keep written records of processing activities, including:

- the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);
- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- where possible, retention schedules; and
- where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal information;
- DPIAs; and
- records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

- the lawful basis for our processing; and
- whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

- carrying out information audits to find out what personal information AHK holds;
- distributing questionnaires and talking to staff across AHK to get a more complete picture of our processing activities; and
- reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

Privacy notice

AHK will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

We will act appropriately to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Individual rights

You (in common with other data subjects) have the following rights in relation to your personal information:

- to be informed about how, why and on what basis that information is processed;
- to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
- to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected

to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

If you wish to exercise any of the rights detailed above, please contact the data protection officer.

Individual obligations

Individuals are responsible for helping AHK keep their personal information up to date. You should let the HR department know if the information you have provided to AHK changes, for example if you move house or change details of the bank or building society account to which you are paid.

You may have access to the personal information of other members of staff, suppliers and clients of AHK in the course of your employment or engagement. If so, AHK expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they might also enjoy the individual rights set out above.

If you have access to personal information, you must:

- only access the personal information that you have authority to access, and only for authorised purposes;
- only allow other AHK staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not AHK staff to access personal information if you have specific authority to do so from the data protection officer;
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in Part 2 – Information Security);
- not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices that are used for work purposes.

You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the special processing conditions being met;

- any data breach;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from AHK's premises without appropriate security measures being in place;
- any other breach of this policy or of any of the data protection principles set out above.

Information security

AHK will use appropriate technical and organisational measures in accordance with the information security policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where AHK uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of AHK;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of AHK and under a written contract;
- the organisation will assist AHK in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist AHK in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to AHK as requested at the end of the contract; and

- the organisation will submit to audits and inspections, provide AHK with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell AHK immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the legal department.

Storage and retention of personal information

Personal information (and sensitive personal information) will be kept securely in accordance with AHK's information security policy.

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data breaches

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

AHK will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

International transfers

AHK may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) on the basis that that country, territory or organisation is designated as having an adequate level of protection (e.g. Privacy Shield), or the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses, or complies with an approved code of conduct.

Training

AHK will ensure that staff are adequately trained regarding their data protection responsibilities, all AHK employees will be required to complete e-learning on data protection and information security. Individuals whose roles require regular access to personal information, who are responsible for implementing this policy, or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Consequences of failing to comply

AHK takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed; and
- carries the risk of significant civil and criminal sanctions for the individual and AHK; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.

Part 2 - Information Security

Definitions

For the purposes of this Policy:

business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of the Company;
confidential information	means trade secrets or other confidential information (either belonging to AHK or to third parties) that is processed by the Company;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Roles and responsibilities

Information security is the responsibility of all staff, all staff must be familiar with this policy and comply with its terms.

AHK's data protection officer (DPO) is in particular responsible for:

- monitoring and implementing this policy;
- monitoring potential and actual security breaches;
- ensuring that staff are aware of their responsibilities; and

- ensuring compliance with the requirements of Regulation (EU) 2016/679, GDPR and other relevant legislation and guidance.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

This policy applies to all staff, including employees, temporary and agency workers, other contractors, interns, volunteers and apprentices.

AHK information covered by this policy may include:

- personal information relating to staff, customers, clients, suppliers;
- other business information; and
- Confidential information.

This policy supplements Part 1 - Data Protection and any other policies and privacy notices relating to the use of the internet, email and communications, social media, instant messaging and document retention and any such relevant policy that may be introduced from time to time, and the contents of those policies must be taken into account, as well as this policy.

We will review and update this policy regularly in accordance with our data protection and other obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy when it is adopted.

General principles

All Company information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

Personal information, and sensitive personal information, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

Staff should discuss with line managers the appropriate security arrangements and technical and organisational measures that are appropriate and in place for the type of information they access in the course of their work.

Company information (other than personal information) is owned by AHK and not by any individual or team.

Company information must be used only in connection with work being carried out for AHK and not for other commercial or personal purposes.

Personal information must be used only for the specified, explicit and legitimate purposes for which it is collected.

Information management

Personal information must be processed in accordance with:

- the data protection principles, set out in Part 1 – Data Protection;
- Part 1 – Data Protection generally; and
- all other relevant policies.

In addition, all information collected, used and stored by AHK must be:

- adequate, relevant and limited to what is necessary for the relevant purposes;
- kept accurate and up to date;

AHK will take appropriate technical and organisational measures to ensure that personal information, confidential information and business information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including but not limited to:

- pseudonymisation of personal information;
- encryption of personal information;
- limiting access; and
- secure physical and electronic storage.

Personal information and confidential information will be kept for no longer than is necessary, stored and destroyed in accordance with AHK's Document Retention Policy.

Human resources information

Given the internal confidentiality of personnel files, access to such information is limited to the HR Department and the Finance department for the processing of payroll. Except as provided in individual roles, other staff are not authorised to access that information.

Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

Staff may ask to see their personnel files and any other personal information in accordance with Regulation (EU) 2016/679, GDPR and other relevant legislation.

Access to offices and information

- Office doors, keys and access codes must be kept secure at all times and keys or access codes must not be given or disclosed to any third party at any time.
- Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows.
- Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to confidential information.
- Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room that contains confidential information, then steps should be taken to ensure that no confidential information is visible.
- At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

Computers and IT

- Password protection and encryption must be used where available on company systems in order to maintain confidentiality.
- Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.
- Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.
- Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of the IT department and must be encrypted. Data held on any of these devices should be transferred to the company's

computer network as soon as possible in order for it to be backed up and then deleted from the device.

- All electronic data must be securely backed up at the end of each working day.
- Staff must ensure they do not introduce viruses or malicious code on to AHK systems. Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact the IT Service Desk for guidance on appropriate steps to be taken to ensure compliance.

Communications and transfer of information

Staff must be careful about maintaining confidentiality when speaking in public places, e.g. when speaking on a mobile telephone.

Confidential information must be marked 'confidential' and circulated only to those who need to know the information in the course of their work for AHK. Communications for internal use only should be clearly marked as such and should never be forwarded to third parties including clients. Further details of how emailed information must be marked and protected are set out in AHK's Email Policy and in the rest of this part.

Confidential information must not be removed from the Company's offices unless required for authorised business purposes, and then only in accordance with this document.

Where confidential information is permitted to be removed from the Company's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

- stored on an encrypted device with strong password protection, which is kept locked when not in use;
- when in paper copy, not transported in see-through or other unsecured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains); and
- not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

Postal, document exchange (DX) and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

Personal email and cloud storage accounts

Personal email accounts, such as yahoo, google or hotmail and cloud storage services, such as dropbox, icloud and onedrive are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.

Do not use a personal email account or cloud storage account for work purposes.

If you need to transfer a large amount of data, contact the IT Service Desk for help.

Home working

Staff must not take Company information home unless required for authorised business purposes, and then only in accordance with this part.

Where staff are permitted to take Company information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

- personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all personal and confidential information must be retained and disposed of in accordance with this policy.

Staff must not store confidential information on their home computers (PCs, laptops or tablets).

Transfer to third parties

Third parties should be used to process confidential information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be processors for the purposes of Regulation (EU) 2016/679, GDPR.

Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the Legal department for more information.

Overseas transfer

There are restrictions on international transfers of personal information. Staff may only transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway, with the prior written authorisation of the Legal department. You should refer to Part 1 – Data Protection for further information on overseas transfers.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided online via e-learning and through seminars or workshops. Completion of training is compulsory.

The Learning and Development department will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our Information management and security policy or procedures, please contact the Learning and Development department.

Reporting breaches

All members of staff have an obligation to report actual or potential confidential information and data protection compliance failures. This allows AHK to:

- investigate the failure and take remedial steps if necessary;
- maintain a register of compliance failures; and
- make any applicable notifications.

Please refer to our Compliance Reporting policy for our reporting procedure.

Consequences of failing to comply with this policy

AHK takes compliance with this policy very seriously. Failure to comply with it puts both staff and AHK at significant risk. The importance of this policy means that failure to comply with any requirement of it may lead to disciplinary action, which may result in dismissal.

Staff with any questions or concerns about anything in this policy should not hesitate to contact the DPO or the Legal department.