BOXING SCOTLAND LIMITED (BSL)
Data Protection Policy

Introduction

Boxing Scotland Limited ("**Company**") obtains, keeps and uses personal information (also referred to as data) about members of our workforce**,** members, suppliers and other third parties during the course of our business activities and we are committed to treating it appropriately and lawfully.

The Company understands that personal information is valuable, important and sensitive and is committed to protecting the privacy and security of all such information and complying with data protection laws. We are also committed to providing clear information about how we obtain and use personal information, and how and when we delete that information once it is no longer required.

This Data Protection Policy sets out how we ensure that the personal information of members of our workforce**,** members, suppliers and other third parties is used, transferred, stored and disposed of appropriately and lawfully.

Its purpose is also to ensure that staff understand and comply with the rules about the collection, use and deletion of personal information to which they may have access in the course of their work.

The Company's Data Protection Officer ("DPO"), Marianne McMahon, is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or for further information, you should contact the DPO **marianne.mcmahon@boxingscotland.org / 0845 2417016**.

If the DPO is unavailable for any reason, please contact the CEO, Fraser Walker, in the alternative. Fraser Walker can be contacted on **fraser.walker@boxingscotland.org /0845 241 7016.**

Scope

This Policy applies to all personal information we process regardless of how that data is stored or whether it relates to past or present employees, job applicants, workers, agency workers, consultants or contractors, interns, apprentices, volunteers, board members, members of Boxing Scotland Limited, clients or supplier contacts, shareholders, website users or any other individual.

This policy gives important information about:

1. the Data Protection Principles with which the Company must comply;
2. what is meant by personal information (or data) and sensitive personal information (or data);
3. how we gather, use and delete personal information and sensitive personal information in accordance with the Data Protection Principles;
4. 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;

5. your rights and obligations in relation to data protection; and

6. the consequences of failure to comply with this policy.

This Policy applies to our entire workforce, including employees, workers, agency workers, contractors and consultants. Where we refer to 'employees' and 'employment' in this Policy, this includes all the categories of our workforce listed above to the extent it is relevant to those individuals.

You must read, understand and comply with this Policy when processing personal information on our behalf. You may also be required to attend training on the areas covered by this Policy.

You should refer to your Data Protection Privacy Notice and our other related policies for further information regarding the protection of personal information in those contexts, and to help you interpret and comply with this Policy.

We will review and update this policy from time to time in accordance with our data protection obligations. It does not form part your contract of employment or other contract to provide services and we may amend, update or supplement it from time to time.

Data Protection Principles

The Company will comply with the following Data Protection Principles when processing personal information. We will:

- process personal information lawfully, fairly and in a transparent manner;
- collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those purposes;
- only process personal information that is adequate, relevant and necessary for the purposes for which it is processed;
- ensure that personal information is accurate and, where necessary, kept up to date, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- keep personal information in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed; and
- 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
- not transfer data to another country without appropriate safeguards being in place.

Lawful reasons 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 reason(s) for that processing, which may be one, or a combination of:
    - that the data subject has consented to the processing (this will only apply in limited circumstances);
    - 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;
    - that the processing is necessary for compliance with a legal obligation to which the Company is subject;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
    - [that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority;
    - that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests or 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) and provide a copy of this to the individual(s) that the information relates to where appropriate;
- where sensitive personal information is processed, also identify a lawful special condition for processing that information (see **Sensitive personal information** below), and document it; and
- where criminal records information is processed, also identify a lawful condition for processing that information, and document it (see **Criminal records information** below).

When deciding whether the Company's legitimate interests are the most appropriate reason 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).

Where you process personal information on our behalf, you must ensure that you comply with the above requirements in order to help the Company meet its obligations.

Sensitive personal information

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

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

- we have a lawful reason for doing so, as set out above, e.g. it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, e.g. the:
    - data subject has given has given explicit consent (this will only apply in limited circumstances);
    - processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;
    - processing is necessary to protect the data subject's vital interests, and the data subject is physically or legally incapable of giving consent;
    - processing relates to personal information which is manifestly made public by the data subject;
    - processing is necessary for the establishment, exercise or defence of legal claims; or
    - processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, you must notify the DPO of the proposed processing, so that they may assess whether the processing complies with the criteria set out 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.

The Company's data protection Privacy Notice(s) sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

We give further information about how long we use sensitive personal information, when it will be deleted and how we safeguard it in this Policy and our related policies and procedures. We will comply with this Policy and our related policies and procedures to ensure that we comply with the Data Protection Principles when we process sensitive personal information.

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

During the recruitment process: the manager responsible for recruitment of the post, with guidance from the DPO, 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 his or her CV or during the interview, where practicable 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 not ask health questions in connection with recruitment

During employment: management, with guidance from the DPO will collect, store and use:

- health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance, managing sickness absence or working capacity and related issues, and facilitating employment-related health and sickness benefits;
- sensitive personal information for the purposes of equal opportunities monitoring

A full list of the sensitive personal information we process may be requested from the DPO.

Criminal records information

We will only collect, store and use information about criminal convictions and offences if it is appropriate, given the nature of your role, and provided we are legally able to do so. Where appropriate, we will process information about criminal convictions and offences as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us or from Disclosure Scotland. Your Privacy Notice gives further details about how we use criminal records information.

Where the Company processes criminal records information, we will follow this Policy and our related policies and procedures to ensure that we comply with the Data Protection Principles.

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 the Company 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 DPO in order that a DPIA can be carried out.

During the course of any DPIA, the employer will seek the advice of the DPO and the views of a representative group of employees and any other relevant stakeholders.

Documentation and records

We will keep written records of certain processing activities which we carry out (organisations employing 250 or more people must keep a record of *all* processing activities they are responsible for under Art. 30 GDPR, but organisations employing less than 250 people only have to keep records of processing which is likely to result in a risk to individuals' rights and freedoms, processing which is not occasional or which involves sensitive personal information or criminal records information), 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 periods; and
- where possible, a description of technical and organisational security measures in place.

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 on data retention and erasure 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.

Privacy Notice

The Company 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 take appropriate measures to provide information in Privacy Notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Whenever the Company first obtains personal information directly from an individual, we must also ensure that an appropriate Privacy Notice is provided to them. When personal information is obtained indirectly (for example, from a third party or publically available source), we are required to provide the individual with certain information as soon as possible after we receive the data. We must also check that the personal information was collected lawfully and on a basis which envisages our proposed use of that information.

You must contact the DPO for further guidance whenever you are obtaining personal data, whether directly or indirectly, in the course of your role, to ensure we comply with our obligations to provide information.

Individual rights

You (as well as 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—see the Company's data protection Privacy Notice;
- 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 — see the Company's Data Subject Access Request Policy;
- 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 listed above, please contact the DPO.

Information security

The Company will use appropriate technical and organisational measures 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 appropriate, 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 the Company 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 should provide that:

- the organisation may only use the personal data for specified purposes and in accordance with our written instructions;
- 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 the Company and under a written contract;
- the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist the Company 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 the Company as requested at the end of the contract; and

- the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company 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 or extended, the relevant staff must seek approval of its terms by the DPO and ensure we are meeting all of our data protection obligations in relation to that information.

Storage and retention of personal information

Personal information (and sensitive personal information) must not be retained in a form which allows the individual that it relates to be identified for any longer than needed for the purposes for which it is being held.

The length of time for which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained and any relevant legal, regulatory or business considerations, and you should follow the Company's Data Retention Guidelines/Records Retention Policy set out at Appendix 1 below which set out the relevant retention periods, or the criteria that should be used to determine the appropriate retention period. Where there is any uncertainty, you should consult the DPO for advice.

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.

You must help the Company comply with its obligations in relation to the storage and retention of personal data by not keeping personal information in a form which enables the identification of the person it relates to for longer than needed for the legitimate business purpose(s) for which we collected it.

You must take all reasonable steps to ensure that personal information is securely destroyed or erased from our systems once it is no longer required. You should consult the *Data Retention Guidelines/Records Retention Policy* and/or contact the DPO to discuss the deletion or erasure of personal information in advance of taking any action.

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.

The Company 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.

If you know or suspect that a data breach has occurred, you must immediately contact the DPO, or if the DPO is not available the CEO of Boxing Scotland Limited on 0845 241 7016 or

fraser.walker@boxingscotland.org. Do not attempt to investigate the matter yourself. You should preserve all evidence relating to the potential data breach.

Failure to report a data breach or suspected data breach immediately and/or a failure to preserve all evidence, may result in disciplinary action being taken against you, up to and including summary dismissal.

International transfers

Personal information is transferred to another country when it is sent, transmitted, viewed or accessed in or to a different country.

The Company may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to Switzerland on the basis that that country is designated as having an adequate level of protection.

There may be other occasions where the Company may need to transfer personal data outside of the EEA. You will be notified of such occasions in advance; along with details of the organisation / destination country and details of the adequacy mechanisms in place to protect your personal data.

If other occasions do arise where the Company envisages transferring personal data outside the EEA, the Company may only do so on the basis that the organisation receiving the information is:

- located in a jurisdiction designated as having an adequate level of protection; or
- has provided adequate safeguards by way of:
    - binding corporate rules;
    - standard data protection clauses; or
    - compliance with an approved code of conduct.

You may only transfer personal information outside the EEA where one of the above conditions applies. Before sending any personal data outside the EEA, you must contact the DPO for advice. Failure to seek advice from the DPO in advance of sending data outside the EEA may result in disciplinary action, up to and including summary dismissal.

Training

The Company will ensure that its workforce is adequately trained on their data protection responsibilities. Individuals whose roles require regular access to personal information, or 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.

Your obligations

You are responsible for helping the Company keep your personal information up to date. You should let management know as soon as possible if the personal information you have provided to the Company 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, board members, suppliers and members of the Company, that we are responsible for, in the course of your employment or engagement or otherwise. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in above. If you do have such access to personal information, you must:

- only access or obtain the personal information that you have a job-related need and authority to access or obtain, and only for authorised and lawful purposes;
- only allow other Company staff to access or obtain personal information if they have a job-related need to access that information, appropriate authorisation and a lawful reason for doing so;
- only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the DPO and suitable safeguards and contractual arrangements have been put in place (see **Information Security** above for more information);

- ensure that the personal information we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it;
- 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 the Company's IT Policy.
- 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;
- not store personal information on local drives or on personal devices that are used for work (or other) purposes;
- comply with this Policy and our related policies and procedures; and
- not keep personal information in a form which enables the individual that it relates to to be identified for longer than needed for the legitimate business reason(s) for which we originally collected it, and comply with our Data Retention Guidelines retention periods.

You should contact the DPO if you have any questions about this or are unclear about your responsibilities.

You should also contact the DPO 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 or criminal records information, without one of the conditions set out above 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 the Company's premises without appropriate security measures being in place;
- personal information being retained for longer than it is legitimately needed for;
- any other breach of this Policy or any of our related policies or procedures, or any of the Data Protection Principles set out above.

Consequences of failing to comply with this Policy

The Company 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 the Company; 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, engagement or appointment terminated with immediate effect.

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

Definitions used in this Policy:

automated decision making takes place when an electronic system uses personal information to make a decision without human intervention;

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 protection impact assessment means tools and assessments used to identify and reduce the risks of a data processing activity;

data subject means the individual that personal information relates to;

legitimate interests assessment or LIA means an assessment of what our legitimate interest is, whether the processing necessary to achieve that interest and balancing this against the individual's interests, rights and freedoms;

personal information (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

Privacy Notice means a notice which sets out the type of personal information that we, as data controller, collect about certain types of individuals (e.g. our workforce), the purposes for which it is collected and how it is handled;

processing 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' or 'sensitive personal data') means personal information about an individual's race or 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.

Appendix 1

Data Retention Guidelines

Introduction

The Company is committed to the efficient and appropriate management of the records it is responsible for, including in respect of the retention of your personal information.

These guidelines set out our approach to data retention. They do not form part of your contract of employment and we may amend or update them, or the recommended retention periods set out in the Schedule below, at any time.

Retention of records

Our general approach is to only retain your personal information for as long as is reasonably necessary to fulfil the purposes for which it was collected by us or provided by you. These purposes are listed in our Privacy notice(s) issued to you and available on request and include for the purposes of satisfying any legal, accounting, or reporting requirements.

The Company is required by law and/or our regulatory obligations to keep certain types of records for a specified minimum period of time. We may also have legitimate business reasons for keeping records for a period of time, which may in some cases exceed any minimum periods which we are required by law or regulatory obligations to keep them for, for example in order to resolve any queries or disputes which might arise from time to time.

Where the Company's records include personal data, we must also comply with the requirements under data protection law that personal data must be kept for no longer than is reasonably necessary for the purposes for which it is processed.

This means that personal data should be securely destroyed or erased when it is no longer required, either to fulfil the purposes for which we collect your personal information or you provide it, to comply with legal or regulatory requirements in relation to record keeping or for legitimate business reasons.

Our standard data retention periods

Our standard data retention periods for HR records are set out in the schedule to this policy.

It is important to note that these are standard retention periods, and there will be times when it is appropriate for us to depart from these periods, including keeping data for a longer period of time than is specified, for example where a legal claim is ongoing and the documents are relevant to that claim.

In setting these standard retention periods, the Company has given careful consideration to the nature, sensitivity and amount of personal data contained in each type of record, the potential risk of harm associated with retaining it (including from it becoming outdated or inaccurate, or from unauthorised use or disclosure of it), the purposes for which it was obtained and any legal, regulatory, professional or legitimate business reasons for retaining it for a particular period of time.

Where there is any uncertainty about retention periods or anything else relating to this policy, you should consult the DPO for advice.

Records will be securely deleted or destroyed after the end of the relevant retention period, unless there is a particular reason for keeping them for longer. In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use that information on an ongoing basis without further notice to you, for example for statistical purposes.

Training

Training is available on the issues covered by this policy. Please contact the DPO for further information.

Further Information

For further information or advice on the content or application of these guidelines, please contact **the Data Protection Officer** who is responsible for data retention.

Schedule: Our standard retention periods for HR records

The table below sets out our standard retention periods in respect of the key categories of HR records held by the Company, which take into account the legal, accounting/reporting and regulatory obligations on the Company and the Company's legitimate business reasons for retaining records for specified periods:

Type of employment record	Standard retention period
Job applications and interview records	Unsuccessful candidates: one year from completion of application process Successful candidates: documents relevant to ongoing employment will be transferred to the individual's personnel file and retained throughout employment and for seven years after employment ends
Criminal record checks	Should be deleted as soon as possible or within a maximum period of 6 months (unless information is assessed as relevant to the individual's ongoing employment, in which case it should be deleted as soon as it is no longer required) If necessary, retain a record of whether the check produced a satisfactory or an unsatisfactory result Once a conviction is spent, it should be deleted unless an exclusion applies
Immigration checks	Two years after the employment ends
Personnel, Appraisal and training records	Generally, records will be kept while employment continues and up to seven years after employment ends, but in some cases a different period will apply
Equal opportunities and diversity monitoring records	Unsuccessful candidates: one year from completion of application process Successful candidates: documents necessary to ongoing employment will be transferred to the individual's personnel file and retained throughout employment and for seven years after employment ends
Employment contracts / written particulars of employment, independent contractor/consultancy contracts and records, changes to terms and conditions	While employment/contract continues and up to seven years after employment/contract ends
Sickness, medical and health records and other absence records	While employment continues and up to seven years after employment ends
Working time records and opt-out forms	For at least two years after the relevant period for records to show compliance with Working Time Regulations 1998 and any working time opt-outs

Type of employment record	Standard retention period
Annual leave records	While employment continues and up to seven years after employment ends
Payroll and salary records	While employment continues and up to seven years after employment ends
PAYE records	Not less than three years after the end of the tax year to which they relate/seven years
Maternity, paternity, adoption and shared parental leave and pay records	While employment continues and up to seven years after employment ends
Parental leave records	While employment continues and up to seven years after employment ends
Current bank details	No longer than necessary
Next of kin/emergency contact details	No longer than necessary
Employee pension schemes	While employment continues and up to seven years after the employment ends 4 years for auto-enrolment opt-out notices
Accident, injury and illness logs and related records	While employment continues and up to seven years after employment ends. In certain circumstances, the Company may be required to keep records for longer
National Minimum Wage records	At least three years beginning with the day upon which the pay reference period immediately following that to which they relate ends
Consents for the processing of personal and sensitive data/special category personal data	While employment continues and up to seven years after employment ends