DATA PROTECTION POLICY

DATA PROTECTION POLICY (EMPLOYMENT)

We obtain, keep and use personal information relating to our workforce for specific lawful purposes, and this policy sets out how we comply with our data protection obligations.

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 workforce, and how and when we delete that information once it is not required.

The person with responsibility for data protection compliance is Ian Ford.

Data protection principles

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

1. we will process personal information lawfully, fairly and in a transparent manner;
2. we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
3. we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
4. we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
5. we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
6. we will take appropriate 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

Before processing of personal information starts and regularly while it continues, we will review the purposes of the processing activity, and select the most appropriate lawful basis for that processing:

1. that the data subject has consented to the processing;
2. 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;
3. that the processing is necessary for compliance with a legal obligation;
4. that the processing is necessary for the protection of the vital interests of the data subject or another person;
5. that the processing is necessary for the purposes of our legitimate interests or those of a third party, except where those interests are overridden by the interests, rights and freedoms of the data subject.

We will check that the processing is necessary for the purpose of the relevant lawful basis, except where the processing is based on consent.
We will document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.

We will include information about the purposes of the processing and the lawful basis for it in our relevant privacy notices.

Where sensitive personal information is processed, we will also identify and document a lawful special condition for processing that information.

Where criminal offence information is processed, we will also identify and document a lawful condition for processing that information.

When determining whether our legitimate interests are the most appropriate basis for lawful processing, we will conduct a legitimate interest's assessment (LIA) and keep a record of it, and if the LIA identifies a significant privacy impact, we will consider whether we also need to conduct a data protection impact assessment (DPIA). We will include information about our legitimate interests in our privacy notices.

Sensitive personal information

We may from time to time need to process sensitive personal information. We will only process sensitive personal information if it is necessary for the performance of the employment contract, to comply with our legal obligations or for the purposes of our legitimate interests; and one of the special conditions for processing sensitive personal information applies:

a) the data subject has given explicit consent;

b) the processing is necessary for the purposes of exercising our employment law rights or obligations or those of 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 establishment, 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 us of the proposed processing, in order that we may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until the assessment 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.

Our data protection privacy notice sets out the types of sensitive personal information that we process, what it is used for and the lawful basis for the processing.
Data protection impact assessments

Where data processing is likely to result in a high risk to an individual’s data protection rights we will carry out a data protection impact assessment (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.

Documentation and records

We will keep written records of data processing activities which are high risk, and which may result in a risk to individuals’ rights and freedoms or involve sensitive personal information or criminal records information, including:

1. our name and details and where applicable, those of other controllers, our representative and DPO;
2. the purposes of the processing;
3. a description of the categories of individuals and categories of personal data;
4. categories of recipients of personal data;
5. retention schedules; and
6. a description of technical and organisational security measures.

As part of our record of processing activities we will document:

1. information required for privacy notices;
2. records of consent;
3. controller-processor contracts;
4. the location of personal information;
5. DPIAs; and
6. records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of the relevant purpose for which the processing takes place.

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

Privacy notices

We 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.

Individual rights

You have the following rights in relation to your personal information:

1. to be informed about how, why and on what basis that information is processed – see our data protection privacy notice;
2. 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;
3. to have information corrected if it is inaccurate or incomplete;
4. to have information erased if it is no longer necessary for the purpose for which it was originally collected or processed, or if there are no overriding legitimate grounds for the processing (“the right to be forgotten”);
5. 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 information to be erased), or where we no longer need the personal information, but you require it to establish, exercise or defend a legal claim; and
6. to restrict the processing of personal information temporarily where you do not think it is accurate (and we are verifying whether it is accurate), or where you have objected to the processing (and we are considering whether our legitimate grounds override your interests).

Individual obligations

You are responsible for helping us keep your personal information up to date. You should let us know if the information you have provided changes.

You may have access to the personal information of other members of staff, suppliers and customers or clients and we expect you to help meet our data protection obligations to those individuals. If you have access to personal information, you must:

1. only access the personal information that you have authority to access, and only for authorised purposes;
2. only allow other staff to access personal information if they have appropriate authorisation;
3. only allow individuals who are not our staff to access personal information if you have specific authority to do so;
4. keep personal information secure;
5. not remove personal information, or devices containing personal information, from our premises unless appropriate security measures are in place to secure the information and the device; and
6. not store personal information on personal devices.

You should contact us if you are concerned or suspect that one of the following has taken place:

1. processing of personal data without a lawful basis for its processing;
2. any data breach;
3. access to personal information without the proper authorisation;
4. personal information not kept or deleted securely;
5. removal of personal information, or devices containing personal information, from our premises without appropriate security measures being in place;
6. any other breach of this policy or of any of the data protection principles.

Information security

We will use appropriate technical and organisational measures to keep personal information secure, and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
1. making sure that, where possible, personal information is processed in such a way that it cannot be used to identify an individual, or encrypted;
2. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. 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
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Storage and retention of personal information

Personal information and sensitive personal information will be kept securely.

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 occur due to loss or theft of data or equipment on which personal information is stored, unauthorised access to or use of personal information by staff or a third party, loss of data resulting from an equipment or systems failure, human error, unforeseen circumstances, deliberate attacks on IT systems, such as hacking, viruses or phishing scams, and fraud where information is obtained by deception.

In the event of a data breach we will make the required report 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. We will 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

We will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

Training

We will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of failing to comply

We take compliance with this policy very seriously. An employee’s failure to comply with any requirement of this policy may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct.
DATA PROTECTION POLICY (CRIMINAL RECORDS)

This policy supplements our data protection policy (employment). It sets out our policy on asking questions about a prospective or existing employee’s criminal record and carrying out Disclosure and Barring Service (DBS) checks.

It shows our commitment to comply with the DBS Code of Practice and our data protection obligations, to treat prospective employees fairly and not to discriminate unfairly against any subject of a criminal record check on the basis of a conviction or other information revealed.

It sets out how we comply with our data protection obligations in respect of criminal records information and seek to protect such information, and to ensure that staff understand and comply with the rules governing the collection, use and deletion of criminal records information to which they may have access in the course of their work.

The person who is responsible for informing and advising us and our staff on our data protection obligations, including in relation to criminal records information, and for monitoring compliance with those obligations is Ian Ford.

We will ensure that all those who are involved in the recruitment process have been suitably trained to identify and assess the relevance and circumstances of offences; and have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders and the Rehabilitation of Offenders Act 1974.

Our policy statement

Having a criminal record will not necessarily bar you from working with us. We will take into account the circumstances and background of any offences and whether they are relevant to the position in question, balancing the rights and interests of the individual, our employees, customers/clients, suppliers and the public.

We will treat all applicants, employees and volunteers fairly but reserve the right to withdraw an offer of employment if you do not disclose relevant information, or if a DBS check reveals information which we reasonably believe would make you unsuitable for the role.

Asking for criminal records information

Before recruiting we will assess whether we are justified in seeking criminal records information for that job role and whether it is appropriate to limit the information sought to offences that have a direct bearing on suitability for the specific job, and whether the information should be verified with the DBS.

The level of criminal records information and DBS check that we are entitled to request will depend on the post for which the prospective employee’s suitability is being assessed.

We will only ask an individual to provide criminal records information in relation to convictions and cautions that we would be legally entitled to see in a DBS check for the relevant post.

If we assess that we should use the DBS to verify criminal records information, we will:
provide the individual concerned with a copy of our data handling policy before asking them to complete a DBS application form or asking for their consent to use their information to access the DBS update service;

make every subject of a DBS check aware of the existence of the DBS Code of Practice and makes a copy available on request;

we will comply with the DBS Code of Practice.

Once criminal records information has been verified through a DBS check, we will:

- give the applicant the opportunity to provide an explanation if there are inconsistencies between the information supplied by the applicant and the information in the DBS certificate;
- make a record that a DBS check was completed and whether it had a satisfactory or unsatisfactory result; and
- delete the DBS certificate and any record of the information contained in it unless, in exceptional circumstances, we assess that it is clearly relevant to the on-going employment relationship. If it is not deleted it will be kept securely for no longer than is necessary, and no more than six months.

We will not seek criminal records information from any source other than the individual concerned or the DBS.

DBS certificate information will be handled and kept in accordance with our policy on handling DBS certificate information.

**Where information is disclosed**

We have a legal duty, when recruiting staff to work in regulated activity with children or vulnerable adults, to check whether they are on the relevant children’s or adults’ barred list. If a prospective employee’s name does appear on the relevant barred list, it would be against the law for us to employ them to work or volunteer with the relevant group.

Where we have concerns about the information that has been disclosed by the DBS, we will discuss them with the prospective employee and carry out a risk assessment. In carrying out a risk assessment, we will take account of:

- the relevance of the conviction or other matter revealed to the position in question;
- the seriousness of the offence or other matter revealed;
- the circumstances of the offence;
- the age of the offence;
- whether there is a pattern of offending; and
- whether circumstances have changed since the offending took place.

**Data handling policy**

We will ensure that DBS certificate information is kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

In accordance with section 124 of the Police Act 1997, we will ensure that certificate information is only passed to those who are authorised to receive it in the course of their duties. We keep a record of all those to whom
certificates or certificate information has been revealed. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

Once the DBS certificate has been inspected, it will be destroyed in accordance with the code of practice.

Certificate information must only be used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Once a recruitment (or other relevant) decision has been made, we will not keep certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints.

If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so.

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means.

**DATA PROTECTION POLICY (DATA RETENTION – EMPLOYMENT)**

This policy supplements our data protection policy (employment). It sets out how long employment-related information will normally be held by us and when that information will be confidentially destroyed.

The person responsible for implementing and monitoring compliance with this policy is Ian Ford.

We will review this policy regularly to check that it is effective.

**Processes**

Hard copy and electronically-held documents and information will be retained for at least the period specified in our records retention schedule.

All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

Hard copy and electronically-held documents and information must be deleted at the end of the retention period.

Hard copy and electronically-held documents and information will be disposed of securely.

**Schedule**

Employment records and information:

1. Rejected job applicant records, including: contact details, application letters or forms, CVs, references, certificates of good conduct, interview notes, assessment and psychological test results.
Retention period: Six months after applicant is notified of rejection.

Application forms should give applicants the opportunity to object to their details being retained.

2. Application records of successful candidates, including: application letters or forms, copies of academic and other training received, references correspondence concerning employment, CVs, interview notes and evaluation forms, assessment and psychological test papers and results.

Retention period: Six years after employment ceases.

3. Criminal records information: criminal records requirement assessments for a particular post, criminal records information forms, the Disclosure and Barring Service (DBS) check forms, DBS certificates.

Retention period: Criminal records requirement assessments for a particular post - 12 months after the assessment was last used. All other information in this category - as soon as practicable after the check has been completed and the outcome recorded unless, in exceptional circumstances, we assess that it is clearly relevant to the ongoing employment relationship in which case, six months.

If we consider it necessary to keep the information for longer than six months, the DBS should be consulted.

4. Employment contracts, including: personnel and training records, written particulars of employment, changes to terms and conditions.

Retention period: Six years after employment ceases, unless document executed as a deed, in which case 12 years after employment ceases.

5. Directors’ service contracts and any variations.

Retention period: Six years from termination or expiry of the contract, unless executed as a deed, in which case 12 years from termination or expiry.

6. Copies of identification documents (e.g. passports).

Retention period: Not less than two years from date of termination of employment.

7. Identification documents of foreign nationals (including right to work).

Retention period: Not less than two years from date of termination of employment.

8. Records concerning a temporary worker.

Retention period: Six years after employment ceases.

9. Employee performance and conduct records, including: probationary period reviews, review meeting and assessment interviews, appraisals and evaluations, promotions and demotions.

Retention period: Six years after employment ceases.
10. Records relating to and/or showing compliance with Working Time Regulations 1998 including: registration of work and rest periods, working time opt-out forms.

Retention period: Two years from the date on which the record was made.

11. Redundancy records.

Retention period: Six years from date of redundancy.

12. Annual leave records; Parental leave records; Sickness records; Records of return to work meetings following sickness, maternity etc.

Retention period: Six years after the end of each tax year.

13. Records for the purposes of tax returns including wage or salary records, records of overtime, bonuses and expenses, Pay As You Earn (PAYE) records, including: wage sheets, deductions working sheets, calculations of the PAYE income of employees and relevant payments.

Retention period: Three years.

14. Income tax and NI returns, income tax records and correspondence with HMRC.

Retention period: Three years after the end of the financial year to which they relate.

15. Records demonstrating compliance with national minimum wage requirements.

Retention period: Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends.

16. Statutory sick pay (SSP) records.

Retention period: Three years after the end of the tax year to which they relate.

17. Statutory maternity, paternity and shared parental pay records, calculations, certificates or other evidence.

Retention period: Three years after the end of the tax year in which the period of statutory pay ends.