Schedule 15 Data Protection Policy

1. About this policy

The Foundation is committed to being transparent about how it collects and uses the personal data of its employees and where applicable its visitors and to meeting its data protection obligations. This policy sets out the Foundation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of employees and former employees, referred to as HR-related personal data and where applicable of visitors. This policy also refers to employees using and/or processing the personal data of visitors or other personal data for the purposes of the Estate. Where personal data is processed as part of someone's role, the Foundation will provide training and set out its required procedures.

The Foundation has appointed the Director of the Foundation as the person with responsibility for overseeing data protection compliance within the Foundation. He can be contacted at enquiry@stanstedpark.co.uk. Questions about this policy, or requests for further information, should be directed to him.

The Foundation encourages its employees to speak to their line managers if they have any concerns about anything relating to data protection.

Definitions

In this policy, the following definitions apply:

"Personal data" is any information that relates to a living individual who can be identified from that information.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

2. Data protection principles

The Foundation processes HR-related personal data in accordance with the following data protection principles:

- The Foundation processes personal data lawfully, fairly and in a transparent manner.
- The Foundation collects personal data only for specified, explicit and legitimate purposes.
- The Foundation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Foundation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Foundation keeps personal data only for the period necessary for processing.
- The Foundation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Foundation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the Foundation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the Foundation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The Foundation will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, -is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems (where applicable).

The Foundation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

3. The rights of Individuals

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Foundation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the Foundation has failed to comply with their data protection rights; and
- whether or not the Foundation carries out automated decision-making and the logic involved in any such decision-making.

The Foundation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual wants additional copies, the Foundation will charge a fee, which will be based on the administrative cost to the Foundation of providing the additional copies.

To make a subject access request, the individual should contact the Office Manager. In some cases, the Foundation may need to ask for proof of identification before the request can be processed. The Foundation will inform the individual if it needs to verify their identity and the documents it requires.

The Foundation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Foundation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Foundation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Foundation is not obliged to comply with it. Alternatively, the Foundation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Foundation has already responded. If an individual submits a request that is unfounded or excessive, the Foundation will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Foundation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Foundation's legitimate grounds for processing data (where the Foundation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Foundation's legitimate grounds for processing data.

To ask the Foundation to take any of these steps, the individual should send the request to the person responsible for this policy (see above).

4. Retention of data

The Foundation will only retain personal information for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, the Foundation will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of that personal data, the purposes for which we process that personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances the Foundation may anonymise personal information so that it can no longer be associated with the subject of the information, in which case we may use such information without further notice. Once a contractual relationship (in the case of employees) or a relationship (in the case of visitors) with the Foundation ends we will retain and/or securely destroy relevant personal information in accordance with applicable laws and regulations.

5. Data security

The Foundation takes the security of HR-related and all other personal data seriously. The Foundation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Foundation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

6. Impact assessments

Where processing personal data would result in a high risk to individual's rights and freedoms, the Foundation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

7. Data breaches

If the Foundation discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner

within 72 hours of discovery. The Foundation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

8. International data transfers

The Foundation will not transfer HR-related personal data to countries outside the EEA.

9. Updating your personal data

Individuals are responsible for helping the Foundation keep their personal data up to date. Individuals should let the Foundation know if data provided to the Foundation changes, for example if an individual moves house or changes their bank details.

10. Individual responsibilities for handling others personal data

Individuals may have access to the personal data of other individuals in the course of their relationship with the Foundation. Where this is the case, the Foundation relies on those individuals to meet its data protection obligations to employees and/or (if applicable) visitors.

Individuals who have access to personal data are required to:

- ensure data is collected, stored and handled appropriately and in accordance with Foundation policies, guidelines and procedures;
- only access data that they have authority to access and only for the specified lawful purpose for which it was obtained;
- not share personal data informally (you must only share data in accordance with Foundation procedures where necessary);
- not to disclose data except to individuals (whether inside or outside the Foundation) who have appropriate authorisation (if unsure seek permission from your line manager;
- keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to make unnecessary copies of personal data. Where copies are made for legitimate purposes, copies should be kept and disposed of securely;
- lock computer screens when away from desks;
- not to remove personal data, or devices containing or that can be used to access personal data, from the Foundation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes;
- ensure personal data is encrypted before being transferred electronically to authorised external contacts. The Office Manager will have more information on how to do this;

- ask for help from the Office Manager if they are unsure about data protection or if they notice any areas of data protection or security the Foundation can improve upon; and
- report data breaches of which they become aware to the Director of the Foundation

Failing to observe these requirements (whether deliberately or negligently) may amount to a disciplinary offence, which will be dealt with under the Foundation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct.

Please note it is a criminal offence to conceal or destroy personal data which is part of a subject access request.

Where your role entails processing of personal data of employees and/or visitors, you must adhere to the procedures and guidelines in place. If you have any queries in relation to the processing of personal data of others and/or related procedures, these must be directed to your line manager immediately so that the appropriate training can be provided.

11. Training

The Foundation will provide training to individuals about their data protection responsibilities if applicable to their role.

Individuals whose roles require regular access to personal data, 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.

12. Breaches of data protection

If you have concerns in relation to data protection rules for the use of personal data you should raise them with the Office Manager.