Key and Community Lifestyles

Data Protection Policy

Introduction

The organisation is committed to being transparent about how it collects and uses individuals' personal data, to ensuring the secure and safe management of data held by it and to meeting all its data protection obligations under current legislation. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

Staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and related documentation.

The organisation needs to gather and use certain information about individuals (also referred to as data subjects). These can include job applicants, employees, people we support, tenants and other individuals that the organisation has a relationship with.

Data Protection Contacts

The Head of HR has the role of Data Protection Manager, the person with responsibility for data protection compliance within the organisation and a point of contact for the Information Commissioner's Office and data subjects. The Data Protection Manager can be contacted at The Square, 70 Renton Street, Glasgow G4 0HT. As of 11 November 2019, Key is deemed to be a Public Authority under the Freedom of Information (Scotland) Act 2002 and is, therefore, required to appoint a Data Protection Officer (DPO) with responsibility for monitoring compliance. We have engaged RGDP LLP (www.rgdp.co.uk) to act as our Data Protection Officer who may be contacted by email at info@rgdp.co.uk

Data Protection Principles

The organisation is a Data Controller in that it decides why data is processed, how it is processed and what happens to the data. The organisation processes personal data in accordance with the following data protection principles and requirements.

We:

- process personal data lawfully, fairly and in a transparent manner;
- collect data for specified and legitimate purposes and do not process data in a manner that is incompatible with those purposes;
- collect data that is adequate, relevant and limited to what is necessary in relation to the
- purposes for which it is processed;
- ensure that data is accurate and kept up to date, and take every reasonable step to rectify or
- erase data that is inaccurate without delay;
- keep data only for the period necessary for the purposes of processing;
- ensure that appropriate security is in place to protect data against unauthorised or
- unlawful processing, accidental loss, destruction or damage;
- process data in accordance with the rights of data subjects; and
- would only transfer data outside the European Union if there was an adequate level of protection
- for the rights and freedoms of data subjects.

In addition, the organisation is accountable and takes responsibility for demonstrating compliance with the above principles.

Data

"Personal Data" is any information that relates to an individual who can be identified either by that data alone, or in conjunction with other data held by the organisation.

"Special Category Personal Data" is sensitive in nature so needs more protection. For example, it may relate to a person's health, ethnic origin, religion or politics.

The organisation manages a significant amount of data, from a variety of sources. This data contains both Personal Data and Special Category Personal Data.

Processing of Personal Data

"Processing" is any use that is made of data including collecting, storing, amending, disclosing or destroying it. The processing of Personal Data is only permitted if justified on one or more of the following lawful bases:

1. Consent: the individual has given clear consent for us to process their personal data for a specific purpose;
2. Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract;
3. Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations);
4. Vital interests: the processing is necessary to protect someone's life;
5. Public task: the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the organisation's official authority;
6. Legitimate interests: the processing is necessary for the purposes of legitimate interests.

Consent

Consent as a ground of processing will only be used where no other alternative ground for processing is available. In that event the consent will be for a specific and defined purpose, be obtained in writing, be freely given and the individual will sign a relevant consent form if willing to consent.

Processing of Special Category Personal Data or Sensitive Personal Data

Processing Special Category Personal Data or Sensitive Personal Data, requires not only a lawful basis but must also be in accordance with one of the following relevant grounds of processing:

The individual has given explicit consent to the processing of this data for a specified purpose;

- Processing is necessary for carrying out obligations or exercising rights related to employment, social security or social protection law;
- Processing is necessary to protect the vital interests of the Individual or of another person, if the individual is incapable of giving consent;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.

Criminal Offence Data
Although not classed as Special Category, criminal conviction/offence data is only permitted if authorised by law.

Data Sharing

The organisation shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with our relevant policies and procedures.

Data Controllers
From time to time we share personal data with third parties who also require to process that data. Both we and the third parties will be processing the data as Data Controllers in their own right so all are bound by the same data protection obligations in law.

Data Processors
A third party organisation that carries out processing of the organisation's personal data on our behalf and on our written instructions is not a data controller but a data Processor. As such we require Data Processors to enter in to an Agreement governing the processing of data, organisational and technical security measures to be implemented and responsibility for breaches.

Data Storage and Security

All Personal Data held by the organisation must be stored securely, whether electronically or in paper format. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

Paper Storage
If Personal Data is stored on paper it should be kept in a secure place such as a locked cabinet so that only those employees who require access to the data to carry out their duties can do so. Employees should make sure that no Personal Data is left where unauthorised members of staff can access it.

Electronic Storage
Personal Data stored electronically must also be protected from unauthorised use and access. Protection is provided in that access to all IT systems is password controlled, access to the network drives is restricted based on each person's role, data stored in network drives is automatically backed up and anti-virus software is installed on every computer.

In addition, members of staff should:

- never disclose their passwords;
- never retain work relating to the organisation and its activities on computers or cloud-based storage systems owned by or subscribed to by employees;
- never bring computers owned by employees into the workplace or connect them to wireless or wired networks belonging to the organisation or the people we support;
- never send personal data to external data processors unless password protected;
- never save information relating to individuals to removable media

Breaches

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is important that all members of staff can identify, know what to do and who to notify about a data breach. Should a data breach occur the DPM must be informed immediately and steps taken to seek to contain the breach by whatever means available.

Reporting and Notification

Based on the information provided, the DPM will consider whether the breach is one which requires to be reported. Breaches which pose a risk to the rights and freedoms of the individuals affected will be reported to the Information Commissioner's Office within 72 hours of discovery. If the data breach is likely to result in a high risk to the rights and freedoms of the individuals, the organisation will notify the affected individuals of the breach.

Recording

All data breaches, whether or not reported to the ICO, will be recorded by the DPM in an internal Breach Register.

Further details are contained in Personal Data Breach Notification Procedure.

Data Subject Rights

As a data subject, individuals have certain legal rights.

It is important that all members of staff can identify and know what to do if approached by an individual who wishes to exercise any of their rights. Requests can be made verbally, they do not require to be in writing so it is important the members of staff can recognise when a request is made. There are strict time limits (normally one month) for responding to such requests so the DPM should be notified immediately.

The right to be informed:

Data subjects have a right to request information about whether or not their personal data is being processed and, if so, how that personal data is being processed.

The individual has the right to be provided with the purpose of the processing; the legal basis of the processing; the categories of personal data being processed; the recipients or categories of recipients to whom we have disclosed or will disclose person data; the retention period for the data (or how we calculate that); the existence of the right to have us rectify, erase or restrict processing of that data; the source of the information if we have not collected the data direct from the individual; the existence of any automated decision making; and the right to lodge a complaint with the ICO.

The organisation provides this information to all data subjects in the form of a privacy notice issued at the point their data is collected.

The right of access:
Individuals have the right to make a request (Subject Access Request) to view their data, whether held in written or electronic form, and be provided with a copy of that data.

The right to rectification:
Where any personal data held is inaccurate, the Individual has the right to require us to rectify the inaccurate personal data.

The right to erasure:
This right is often known as “the right to be forgotten”. Certain conditions must be met, the main two being where the personal data is no longer necessary for the purpose for which it was collected or processed; or where the individual’s consent to processing is withdrawn.

Right to restrict processing:
Individuals are entitled to ask us to restrict the type of processing which is carried out by the organisation.

Right to data portability:
In very limited circumstances, individuals are entitled to request a copy of their personal data for the purposes of transferring it to another data controller.

Right to object:
Individuals have the right to object to their data being processed, on grounds relating to their particular situation, where their personal data is processed based on the public interest or in the
exercise of official authority; or where we are processing their personal data based on legitimate interests.

Rights related to automated decision making including profiling
In certain circumstances individuals are entitled to object to any automated decision making (i.e. without any form of human intervention) which takes place concerning
them.

Full details about these rights, the conditions which apply to them and our procedure for responding are contained in the Data Subject Rights Procedure.

Staff Responsibilities: Confidentiality

In addition to a number of other responsibilities outlined in this policy, members of staff have a contractual duty of confidentiality and have a responsibility to keep secure any personal data to which they may have access in the course of their duties. They must access only data that they have authority to access and only for authorised purposes and must not disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation. If in doubt, the member of staff should consult their line manager or the DPM. The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process. Significant or deliberate breaches of this policy will be investigated under the disciplinary procedure.

Data Protection Impact Assessments

A data protection impact assessment (DPIA) is a process to help the organisation identify and minimise the data protection risks of a project.

In the event that any processing would pose a high risk to individuals' rights and freedoms, the organisation will carry out a data protection impact assessment. The level of risk will take into consideration both the likelihood and the severity of any potential impact on individuals. The DPIA 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.

Archiving, Retention and Destruction of Data

The organisation will not keep personal data for any longer than is necessary for the purposes for which the personal data are processed. We will ensure that all personal data is archived or securely destroyed/deleted in accordance with the periods specified in the Data Retention Schedule.

Documentation

Under data protection law, the organisation must document our processing activities, including our processing purposes, data sharing and retention periods.

We conducted and maintain a detailed data audit which comprises a record of all personal data processed by the organisation together with the relevant processing activities. This includes the data subject; the type, format and source of data; documents used to collect the data; the legal basis for processing; the basis for processing special category data and criminal conviction data; the processing purpose; internal and external data sharing; how the data is stored; security measures; updating; and retention.

These records are held electronically and will be reviewed regularly to ensure they are kept up to date.

Other documentation referred to in this policy including this policy itself will be reviewed and updated on a regular basis.