Human Resources

Data Protection Policy

IMS-HRD-012

Version: 1.00

2016-02-020

Data Protection Policy

1. Index

Data Protection Policy

Data Protection Policy

2. Introduction

For the purposes of this policy Kibble Education and Care Centre and all associated companies will be referred to as Kibble.

- This policy establishes and formalises the approach for ensuring personal information is properly processed, managed and protected in accordance with the requirements of the Data Protection Act 1998. This includes all personal data held, maintained and used in all locations and in all formats (paper and electronic including emails).

- Kibble is committed to the principles detailed in the Data Protection Act and additionally recognises the need to balance the rights of individuals with the operational requirements of Kibble to ensure the safety of individuals within its care.

3. Scope

This policy applies to all services within Kibble and all associated companies.

- The policy covers all personal data held, maintained and used in all locations and in all formats (paper and electronic including emails).
- The policy applies to all Kibble staff, volunteers, contractors and consultants that access and/or use Kibble information.
- The policy includes and covers any data sharing agreements current or future.
- The policy applies to all third parties, current or future, that process, manage or store personal data on Kibble's behalf.

4. Aim

The aim of this policy is to clearly communicate the various controls Kibble has in place to ensure compliance with the Data Protection Act 1998 and all supporting/complimentary legislation.

Data Protection Policy

5. Roles and Responsibilities

This policy details specific responsibilities in relation to compliance with the Data Protection Act 1998.

5.1 The Board of Kibble

The board of Kibble is responsible for all governance within Kibble.

5.2 The Senior Management Team

The Senior Management Team has responsibility for information governance. This involves providing high-level support to ensure that each service applies relevant information governance policies and controls, including compliance with the requirements of the Data Protection Act 1998.

5.3 The Data Protection Officer

The Data Protection Officer is responsible for:

- Acting as the first point of contact for all data protection issues
- Providing guidance and advice on data protection issues
- Renewing and amending Kibble's data protection notification to the ICO
- Co-ordinating, processing and responding to all subject access requests
- Overseeing all data sharing protocols and agreements
- Creating, maintaining and renewing training modules and toolkits as appropriate
- Providing data protection training and awareness raising
- Co-ordinating and investigating information breach procedures

5.4 Department/Line Managers

Department/Line Managers are responsible for ensuring that this policy and any associated procedures governing the use of personal information are in place understood and followed by all staff within their service. In addition they must:

- Ensure that their staff has access and resources to receive data protection training appropriate to their role
- Report any suspected breaches of confidentiality or information loss to the Data Protection Officer and follow any subsequent procedures
- Identify any existing or emerging information risks relating to personal information and report to the Data Protection Officer
- Ensure that personal data required to answer a subject access request is provided timeously to the Data Protection Officer

- Ensure that there are appropriate procedures and measures in place to protect personal data, particularly when that information (hardcopy and electronic) is removed from Kibble's premises
- Undertake annual information self-assessments to ensure on-going compliance with this policy
- Consult the Senior Management Team and Data Protection Officer before entering into any information sharing protocol or agreement

5.5 Employees

Employees have a responsibility for data protection and must:

- Read, understand and follow this policy and any associated procedures that relate to the use and handling of personal information in the course of their work
- Undertake data protection training and ensure they have a clear understanding of their responsibilities when using and handling personal information
- Identify and report any risks to personal information to their line manager and/or the Data Protection Officer
- Identify and report suspected breaches of confidentiality or compromised personal data to their line manager and/or the Data Protection Officer
- Identify and forward any subject access requests to the Data Protection Officer to ensure that requests can be processed in accordance with the statutory timescales
- Assist clients in understanding their information rights and Kibble's responsibilities in relation to data protection

6. Definitions

The definitions below cover terms used within the policy.

In Scotland the Procurator Fiscal has the power to bring criminal proceedings for an offence under the Data Protection Act 1998. The offences under the Data Protection Act 1998 are:

- Processing without a valid Notification;
- Failure to advise the Information Commissioner of changes to the Notification
- Failure to comply with an Information Notice;
- Failure to comply with an Enforcement Notice
- Unlawfully obtaining or disclosing personal data
- Procuring the disclosure of personal data
- Unlawfully selling personal data
- Enforced subject access

6.1 Data Controller

A legal person or organisation who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation. Data controllers can process personal data jointly with other data controllers for specified purposes. Kibble is recognised as a data controller.

6.2 Data Processor

A person, other than an employee of Kibble, who processes personal data on behalf of Kibble. This processing must be evidenced in a written contract. The data processor can only use personal data under the instructions of Kibble for the agreed purposes. Full responsibility for the actions of the data processor in relation to the personal data is retained by Kibble.

6.3 Data Protection Act 1998

The Data Protection Act 1998 gives effect in the UK law to the EC Directive 95/46/EC and came into force on 1 March 2000 repealing the Data Protection Act 1984. The Data Protection Act 1998, together with a number of Statutory Instruments, requires data controllers to comply with the legislation governing how personal data is used for statutory and business purposes. Amendments have also been created by other legislation such as the Freedom of Information Act 2000. It gives rights to individuals in relation to how organisation can use their personal data.

Data Protection Policy

6.4 Data Subject

A living individual who can be identified from the personal data or from additional information held, or obtained, by Kibble.

6.5 Enforcement Notice

The Information Commissioner has the power to serve an enforcement notice on a data controller if they determine that a data controller has failed to comply with the requirements of the Data Protection Act 1998. The Notice sets out the actions that the data controller must take to achieve compliance. A data controller can lodge an appeal against the Notice to the Information Tribunal. If the data controller fails to comply with a valid Enforcement Notice this is a criminal offence under the Data Protection Act 1998.

6.6 (The) Information Commissioner

The Information Commissioner is responsible for the regulation of the Data Protection Act 1998 throughout the UK. The Information Commissioner is appointed by the Queen and is independent of the UK Government.

6.7 Information Notice

An Information Notice can be issued by the Information Commissioner which requires a data controller to provide their office with information that they require to carry out their functions. Failure to comply with an Information Notice is a criminal offence.

6.8 Information Security

Ensures that the information Kibble holds is not compromised by unauthorised access, modification, disclosure or loss.

6.9 Information Sharing

Ensures that Kibble information is shared in a compliant, controlled and transparent manner within the terms of a data sharing agreement.

6.10 Mandate

Provides authorisation for the release of personal data in line with the provisions of the Data Protection Act 1998.

Data Protection Policy

6.11 Notification

Kibble is required to notify the Information Commissioner about the categories of personal information it processes and the purposes the personal information is being processed for. Failure to Notify is a **criminal offence**. Kibble must inform the Information Commissioner of any changes to the processing of personal data and renew the Notification annually. Failure to do so is also a **criminal offence**. The Information Commissioner maintains, and publishes, a Register of Data Controllers.

6.12 Personal Data

Personal Data is information about a living individual who can be identified from that information or from additional information held, or obtained, by Kibble. Examples of personal data are contained in paper files, electronic records and visual and audio recordings.

6.13 Processing

Processing is all actions relating to personal data. Gathering, recording, analysing, amending, using, sharing, disclosing, storing and destroying personal data are all covered by this definition.

6.14 Sensitive Personal Data

Sensitive Personal Data requires a higher level of consideration. The following categories are defined as 'sensitive personal data' for the purposes of the Data Protection Act 1998 –

- Racial or ethnic origin of the data subject
- Political Opinions
- Religious or similar beliefs
- Trade Union membership
- Physical or mental health or condition
- Sexual life
- Criminal offences or alleged criminal activity (and any criminal proceedings).

6.15 Subject Access Request

The right given by the Data Protection Act 1998, to an individual to ask Kibble for a copy of the personal data being processed by Kibble; however, there are exemptions that may be applied in certain circumstances. When granted copies of all the requested personal data will be provided in response to the specific request. The information must be supplied in an intelligible form and in a permanent form unless this would involve disproportionate effort or if the individual agrees otherwise. Kibble recognises the requirements under the Equalities Act 2010 when providing personal data to an individual who may require the information to be provided in a certain format to take a special need into account.

6.16 European Economic Area

Provides for the free movement of goods and persons through member states of the European Union and three of the member states of the European Free Trade Association (Iceland, Liechtenstein and Norway)

Data Protection Policy

7 Policy Introduction

To ensure Kibble offers and delivers relevant and appropriate services to our clients, Kibble will gather and process personal data about our clients/employees/volunteers and other individuals associated with Kibble.

Kibble is listed as a data controller with the ICO and subsequently has listed all types of personal data processed by Kibble and the purposes we use this data for. In addition it states any third parties with whom the information may be shared with. Kibble's registration number is **Z5968316** and Kibble's full registration details can be found on the ICO website**, http://www.ico.gov.uk/.**

The Data Protection Act 1998 sets out 8 principles which must be complied with when processing personal data. These are:

7.1 (Principle 1) Processing Personal Data Fairly and Lawfully

Kibble regularly collects personal data on individuals we support or have a relationship with (e.g. suppliers, employees). In accordance with the conditions set out in the Data Protection Act 1998, Kibble will ensure that there is a fair and lawful basis for collecting and processing personal data. Kibble will ensure that the data is not used in such a manner to unjustified adverse effects on the individuals concerned.

Kibble will be transparent about how it intends to use the data, and give individuals appropriate privacy notices when required for collecting their personal data.

7.2 (Principle 2) Processing Personal Data for Specified Purposes

Kibble will explain why it is collecting personal data and how it intends to use that data. An annual review of personal information gathering forms and methods used to gather information will be undertaken by Data Protection Officer to ensure legal compliance. The guidance provided by the Information Commissioners Office covering the *Code of Practice on Privacy Notices: (https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf)* is used to support the compliance process.

To provide clients with a better service, personal data collected across Kibble services may be used in different ways form its original intention, if its use is deemed appropriate and fair, clients will be advised their personal data is to be used in a new way.

7.3 (Principle 3) The Amount of Personal Data you may hold

Kibble will only obtain, use and retain personal information that it actually needs to support its business and operational requirements. The information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is intended.

7.4 (Principle 4) Keeping Personal Data Accurate and up to date

Kibble will ensure that personal data is accurate, relevant and current to facilitate the effective delivery of services. The Data Protection Act 1998 recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. So the Data Protection Act 1998 makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties. To comply with these provisions you should:

- Take reasonable steps to ensure the accuracy of any personal data you obtain
- Ensure that the source of any personal data is clear and referenced
- Carefully consider any challenges to the accuracy of information
- Consider whether it is necessary to update the information

7.5 (Principle 5) Retaining Personal Data

Kibble will ensure that personal data is retained and disposed of in accordance with Kibble's Record Management Plan and Retention and Disposal Schedule. Retention rules apply to both hardcopy and electronic formats. All personal data will be disposed of securely and appropriately by a registered Confidential Waste Management contractor.

7.6 (Principle 6) Personal Data Shall be Processed in Accordance with the Rights of Data Subjects

7.6.1 Subject Access Requests (Requests for Personal Information)

Section 7 of the Data Protection Act 1998 gives individuals or advocates acting on their behalf, (providing proof of authorisation can be provided and verified), the right to ask what personal information is held about them, and to obtain a copy of that information, subject to limited exemptions.

Subject access requests are processed by the Data Protection Officer and must be responded to within 40 calendar days. If an individual believes Kibble has not complied with the Data Protection Act 1998, they can refer their concerns to the Information Commissioner's Office and ask them to undertake an assessment of how Kibble has dealt with their request.

The Data Protection Act 1998 gives data controllers the right to charge a fee of £10.00 (the fee can be higher for different types of records, such as school records). Kibble reserves the right to charge for compliance with Subject Access Requests as laid out by the Data Protection Act 1998.

Data Protection Policy

7.6.2 Freedom of Information Requests

At Present Kibble is not subject to the legal requirements of FOI or FOISA; however, in the interest of best practice where applicable Kibble will attempt to provide the requestor with information providing this does not lead to a breach the Data Protection Act.

7.6.3 Prevention of Processing Causing Damage or Distress

Individuals can ask Kibble, in writing, to stop using their personal data if they consider that the processing of their data is causing them substantial unwarranted damage or distress. The individual is not entitled to serve such a notice if any of the following conditions for using their personal information apply:

- The individual has given a valid consent to the use of their personal information
- The use of the personal information is required for the purpose of a contract with the individual
- The use of the personal information is necessary for any legal obligation placed on Kibble
- The use of the personal information is necessary to protect the vital interest of the individual
- Kibble must respond within 21 calendar days if a notice to cease using personal information is received.

7.6.4 Right to Rectification, Blocking, Erasure and Destruction of Personal Data

- An individual has the right to have any inaccurate personal data corrected, blocked, erased or destroyed in circumstances where the personal data is inaccurate.
- If individuals disagree with a professional opinion which has been recorded about them, a note will be added to their record.

7.6.5 Rights in Relation to Automated Decision Making

An individual is entitled to ask Kibble in writing, that any decision which has a significant effect on them is not based solely on automated decision making methods. At present Kibble does not use any automated decision making models.

7.6.6 Rights to Compensation

An individual who suffers damage or distress as the result of contravention of the Data Protection Act 1998 by Kibble may seek compensation by application to the Court.

7.7 (Principle 7) Information Security

Kibble has in place appropriate security measures to prevent the personal data it holds being accidentally or deliberately compromised. Personal data must be kept secure at all times. Kibble's Record Management Plan, Retention and Disposal Schedule, ICT Policies on Workstation Security and Email and Internet usage will provide support and practical advice that must be followed to protect all personal data in possession of Kibble.

7.7.1 Data Breaches

Data breaches can occur through the theft or accidental loss of personal data (for example, laptops, tablets, portable devices, files containing personal data). It can also occur through the unauthorised use or accidental disclosure of personal data by employees, and deliberate attacks on Kibble systems.

All breaches involving personal and sensitive personal data must be reported to the Data Protection Officer immediately. This will allow Kibble to take all the necessary steps to recover the data and limit any potential damage caused by the breach. An investigation into the circumstances and consequences of the breach will be carried out by the Data Protection Officer in line with the Kibble's Data Security Breach Management Policy.

7.8 (Principle 8) Personal data shall not be transferred outside the EEA without suitable and appropriate safeguards

While Kibble does not routinely transfer personal information outside the United Kingdom and the European Economic Area, there may be occasions when this required. The Data Protection Officer will advise and ensure that there are appropriate safeguards in place to satisfy the 8th principle.

8. Policy Information

8.1 Disclosure of Personal Information

There are many instances where personal data can be disclosed with (and without) the consent of the individual or with their consent through a mandate. On any such occasions, only the personal data that is necessary should be disclosed. When considering the disclosure of information attention must be given to the purpose of the request for information which may include ensuring the safety and wellbeing of clients. All requests for disclosure which fall out with business as usual requests (covered further below) should follow the procedure detailed in Information Request Flowchart and in all instances the Data Protection Officer should be made aware of them before the release of information is carried out.

8.2 Business as Usual Requests

If an individual requests personal data that has already been sent or disclosed to that individual (for example, a letter that has been sent previously), then services should treat such requests as business as usual requests and send replacement copies, subject to confirming proof of identity.

If partner agencies request information on clients that has previously been agreed or is included in contracts or placement agreements, this information should be treated as business as usual requests and complied with utilising the most secure method of providing this information, subject to confirming proof of identity. This relates to live information readily available in the electronic or hard copy casefile, requests for information which is not readily available should follow the guidance in the Information Request Flowchart.

8.3 Disclosure of Personal Data Relating to Crime and Taxation

Section 29 of the Data Protection Act 1998 allows Kibble to consider disclosing personal data for the purpose of prevention or detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of taxes or duties. Each request is considered on a case by case basis and must be forwarded to the Data Protection Officer and Senior Management Team for processing and response.

8.4 Disclosure of Data Required by Law

Section 35 of the Data Protection Act 1998 allows Kibble to consider releasing information in relation to legal proceedings. Each request is considered on a case by case basis and must be forwarded to Data Protection Officer and Senior Management Team for processing and response.

8.5 Unauthorised Disclosure

Employees (and all others covered by this policy) must never disclose personal data obtained in the course of their work with Kibble, or access personal data without appropriate permissions. It is a criminal offence under section 55 of the Data Protection Act 1998 to knowingly obtain or disclose personal data without the consent of the data controller (Kibble).

8.6 Data Sharing

Kibble works with other public agencies to provide services and support our clients. The sharing of personal data between Kibble and other public authorities will be subject to formal data sharing protocols which set out overarching common rules adopted by Kibble and other public agencies with whom it wishes to share data. Details of each data sharing process are documented in data sharing agreements. A central register of all protocols and agreements will be maintained by the Data Protection Officer to ensure that transfer and sharing arrangements meet the requirements of the Data Protection Act 1998, and the Information Commissioner's Code of Practice on Data Sharing: (https://ico.org.uk/media/about-the-ico/consultations/2069/data_sharing_code_of_practice.pdf). All new data sharing protocols and agreements must be agreed by the Senior Management Team and the Data Protection Officer before implementation.

8.7 Data Processing

Consultants may carry out work and process personal data on Kibble's behalf to help deliver services. In such cases, Kibble remains the 'data controller' responsible for that personal data, and the consultant as the 'data processor' who processes that data on behalf of Kibble. Such arrangements must be governed by written agreements or contracts to ensure compliance with this policy and the data protection principles, including on-going monitoring. The Senior Management Team and the Data Protection Officer must be consulted before engaging consultants who process personal data.

8.8 Notification

As a Data Controller, Kibble has to notify the Information Commissioner about the types of personal data it collects and processes. Kibble's notification is included on the Data Protection Register which is available on the Commissioner's website. The Data Protection Officer is responsible for compiling and renewing Kibble's notification each year. It is a criminal offence not to notify the Information Commissioner, if there is a requirement to do so. Failure to maintain an up to date notification, if required to do so, is a criminal offence.

8.9 Information Asset Register (To be decided if relevant or not)

An Information Asset Register will be maintained by the Data Protection Officer. The register identifies personal data and sensitive personal data held by Kibble, and helps to evaluate and assure compliance with Kibble's policies and processes.

8.10 Training

All employees, contractors, consultants and volunteers need to be aware of their obligations under the Data Protection Act 1998. A variety of training methods will be employed to ensure appropriate levels of awareness, understanding and knowledge.

9 Related Documents

Data Protection Act 1998
Freedom of Information Act 2000
Freedom of Information (Scotland) Act 2002
Equalities Act 2010
Kibble Record Management Plan
Kibble Retention and Disposal Schedule
Kibble Workstation Security Policy
Kibble Email and Internet Usage Policy
ICO Code of Practice on Privacy Notices
ICO Code of Practice on Data Sharing

10 Equalities Impact

There is no adverse impact on any group in terms of race, religion, disability, ethnic origin, sexuality or age in relation to this policy. The Act includes clauses relating to information about young children and secondary legislation provides legislative grounds to be followed when dealing with personal information about people who have a limited capacity as to the understanding of their rights under the Act. Secondary legislation also provides clauses to ensure compliance with specific categories of information such as adoption and education records.

11 Risk Assessment

Failure to comply with any requirement of the Act could result in enforcement action by the ICO. The ICO has powers to impose a Civil Monetary Penalty which can result in a fine of up to £500 000 for each breach. This amount could rise considerably subject to the adoption of the Data Protection Regulation under consideration by the European Parliament.

- Individuals may take action against Kibble through the Court for any misuse of their personal information. Depending on which Court takes the action fines could be unlimited
- Failure to renew or amend Kibble's Data Protection Notification as required by the Act will result in a criminal offence.
- Failure to respond to any of the time critical response requirements in relation to information rights for individuals will result in a breach of the Act
- Mishandling of personal information will have a serious reputational impact to Kibble
- Mishandling of personal information may have serious implications to one, or more, individuals
- Personal information that is inaccurate or out of date may result in a serious negative impact on one or more individuals

12 Review

This policy will be reviewed annually or more quickly if required by significant changes in legislation, regulation or business practice. It will be reviewed by the Data Protection Officer and presented to the Senior Management Team for ratification.