Data Protection Policy

This policy was agreed by the Trust Board on 19 December 2017 to be used as an interim policy by Sandwell Children's Trust.

The intention is to review this policy by 1 July 2018 to ensure that it is fit for purpose for the Trust.

Sandwell Children's Trust

Information Management Unit

Data Protection Policy

Tier 1 Policy

Version: v1-0 Final

Date Issued: 2014

Document Control

Owning organisation	Sandwell Council
Title	Data Protection Policy
Author	James Trickett
Protective Marking	IL0: UNCLASSIFIED
Review Date	May 2016

Revision History

Revision Date	Editor	Previous Version	Description of Revision
23rd April 2014	James Trickett	n/a	Final version

Document Distribution

Please note – once printed, this documented is uncontrolled. The latest version will always be found on the Council's intranet.

Document Approvals

Approval required	Date approved
JCP	25th March 2014
Leader Decision Making Session	23rd April 2014

Contents

1. Introduction

1.1 The Data Protection Act 1998 implements the European Data Protection Directive in the UK. The Act applies to personal information processed, in this case, by the Council. For the purposes of this Policy, the Council is known as the Data Controller.

1.2 Sandwell Council is fully committed to complying with the Data Protection Act 1998 (DPA). The Council will implement procedures to ensure that all employees, elected members, contractors, agents, consultants and other partners of the Council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the DPA.

1.3 Failure to comply with the Data Protection Act can lead to enforcement action being taken by the Information Commissioner against the Council including a fine of up to £500,000 for each breach.

2. Statement of Policy

2.1 In order to operate efficiently, Sandwell Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, whether it be on paper, in computer records or recorded by any other means.

2.2 Sandwell Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

3. The Principles of Data Protection

3.1 The Data Protection Act requires anyone processing personal data to comply with **Eight Data Protection Principles**. These Principles are legally enforceable.

3.2 The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

4. Shall be accurate and where necessary, kept up to date;

5. Shall not be kept for longer than is necessary for that purpose or those purposes;

6. Shall be processed in accordance with the rights of data subjects under the Act;

7. Shall be kept secure i.e. protected by an appropriate degree of security;

8. Shall not be transferred to a country or territory outside the European Economic Area, unless adequately protected.

3.3 The DPA provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "sensitive" personal data**.

3.4 Personal data is defined as data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data

controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

3.5 Sensitive personal data is defined as personal data consisting of information including:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

4. Handling of Sensitive / Personal Information

4.1 Sandwell Council will, through appropriate management, creation of procedures and the use of strict criteria and controls:-

- Observe fully, conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act;
- The right to be informed that processing is being undertaken;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as inaccurate information.

- The right of access to one's personal information within the statutory 40 calendar days, known as a "Subject Access Request" (SAR). The Council has created and implemented Subject Access Procedure which must be followed by all Officers when handling requests. The Council will also ensure that relevant employees are sufficiently trained to handle requests.

4.2 The Council will not, by default, levy the £10 charge for a SAR. However it does reserve the right to charge the fee if:

1. The requester (data subject) has made a request within the previous 12 months;
2. Responding will place a significant burden on the Council.

4.3 The Council will "stop the clock" against the 40 calendar day response time if the fee is charged.

4.4 A fee will not be levied beyond 15 days of the request being made;

4.5 The Council will follow processes to adequately verify the individual making a Subject Access Request. This might include the requirement to provide:

- A current driving licence
- Current passport
- Birth certificate

4.6 If a request is being made on behalf of a 3rd party, the Council will require written authorisation from the Data Subject to ensure this is a valid request;

4.7 The Council will "stop the clock" if further information or clarification is requested concerning the request. It will not restart until the clarification is received;

4.8 In addition, Sandwell Council will ensure that:

- There is someone with specific responsibility for both Data Protection and Information Security within the organisation;

- Everyone managing and handling personal information understands that they are contractually responsible for following good Data Protection practice;
- Everyone managing and handling personal information is appropriately trained;
- Everyone managing and handling personal information is appropriately supervised;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with regard to handling personal information is regularly assessed and evaluated, via internal and external audits and other means:
- Regular Data sharing with partners will be carried out under a written agreement, setting out the scope and limits of the sharing.
- That where the Council elects to use a third party to process its data (data processor) it will ensure that such processing is undertaken in accordance with a written agreement
- All Elected Members are to be made fully aware of this policy and of their duties and responsibilities under the Act e.g. when acting on behalf of the Council;
- Assessment of the privacy impact from new projects or changed / new processes will be undertaken appropriately using defined Privacy Impact Assessment procedures.

4.9 All managers and officers within the Council's service areas will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that the Council's Information Management Unit is informed of any incidents involving personal information being compromised e.g. lost or sent to the wrong recipient.

4.10 All contractors, consultants, partners or other servants or agents of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in

and are aware of their duties and responsibilities under the DPA. Any breach of any provision of the DPA will be deemed as being a breach of any contract between the council and that individual, company, partner or organisation;

- Allow Data Protection audits by the Council of data held on its behalf (if requested);
- Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

4.11 All contractors who are users of personal information supplied by the Council will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the Council.

5. Implementation

5.1 The Council's Information Management Unit will develop and update procedures and provide training to ensure that the Council meets the requirements of the Data Protection Policy. The Council will also operate a Corporate Information Governance Group to ensure that this policy and accompanying procedures are implemented corporately.

6. Roles and Responsibilities

The Council will ensure specific roles and responsibilities are created and maintained to ensure compliance with this Policy and the DPA.

6.1 Chief Executive

- The Chief Executive has overall accountability and responsibility for ensuring the DPA is complied with by the Council;

- The Chief Executive will delegate responsibility for compliance (including implementation of this policy and other supporting Policies of the Council's Information Governance Framework)

6.2 Corporate Information Governance Group (CIGG)

- CIGG will contribute to the definition of Council Policy in respect of the DPA;

- Members of CIGG will ensure their respective service areas are appraised of this Policy and compliance requirements.

6.3 Senior Information Risk Owner (SIRO)

- The SIRO will lead and foster a culture that values, protects and uses information for the benefit of both the Council and its service users;

- The SIRO has overall responsibility for ensuring that information threats and information security / Data Protection breaches are identified, assessed and managed;

- The SIRO will ensure that the Chief Executive and Management Board are aware and appraised of key information risks.

6.4 Information Management Unit

- The Information Management Unit (IMU) will act as a point of contact for specialist DPA advice and guidance;

- The IMU will prepare and maintain relevant policies, procedures, training and guidance relevant to the implementation and compliance of the DPA throughout the Council;

- The IMU will ensure that the Council maintains its notification to the ICO and will act as the key contact point between the ICO and the Council.

6.5 Caldicott Guardians

- The Caldicott Guardians for Social Care (adults and childrens) will ensure the adequate safeguarding of

personal information processed in connected with social care work ensuring service user information is securely protected and shared where appropriate;

- Caldicott Guardians will act as the link between social care activities, the IMU and CIGG ensuring policies and procedures are embedded within their service areas.

6.6 Service Areas and Information Asset Owners

- Each Service Area will nominate an appropriate Information Asset Owner (IAO) to undertake Information Governance processes and activities are deployed within their service;

- The IAO will undertake and co-ordinate tasks in conjunction with CIGG and the IMU e.g. information asset registers, data sharing audits etc.

6.7 Managers

- Managers are responsible for ensuring their Officers are informed of this Policy plus the supporting procedures and provide adequate time to read them and undertake appropriate training offered by the Council. They must ensure their Officers understand and adhere to Policy and supporting procedures whilst undertaking their work functions;

- All Managers must inform the Information Management Unit of any security incidents, data losses or other DPA breaches;

- Managers must ensure that their Officers undertake all relevant information governance training related to Data Protection including refresher training where appropriate.

6.8 Officers and Employees

- All Officers and Employees (permanent, temporary or contract) of the Council have a responsibility for abiding by the DPA and are required to read, understand and

accept this Data Protection Policy and any supporting procedures;

- All mandatory training offered must be taken up whilst appropriate, relevant additional training must also be considered e.g. SAR training for Officers routinely involved with the handling of such requests;

- All Officers and Employees must handle Subject Access Requests inline with Council procedures;

- All Officers or anyone given legitimate access to Council information must report actual or suspect security incidents, data losses, breaches of the DPA to their Line Manager and/or Information Asset Owner. They are also entitled to report concerns of actual or suspected incidents to the Information Management Unit.

7. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The process to register is referred to as “notification”. Sandwell Council holds a current notification with the Information Commissioner.

The DPA requires every data controller who is processing personal information, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The Council’s Information Management Unit will ensure that the Council’s Notification is kept up to date.

The Council’s registration number is: Z6787899.

8. Monitoring Compliance

Compliance with this Policy will be monitored by CIGG through reporting from the IMU.

Audit Services will provide a review of compliance through their annual audit programme selecting various controls on which to report.

The IMU will review all reported incidents (security incidents, data losses etc) to ensure robust compliance with this Policy.