# DATA PROTECTION POLICY

## May 2018



Updated May 2018
Review May 2019

**St Elizabeth's**

**Data Protection Policy**

## 1.0 Aims and Scope

1.1 Handling information properly is recognised as important to help St Elizabeth's to achieve its aims and objectives and to build good relations with individuals. Mishandling data can have serious repercussions for individuals and for an organisation and can lead to damaged relations, financial penalties and loss of business. St Elizabeth's is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act, 1998 (DPA). This policy sets out arrangements to comply with this legislation.

1.2 The DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. 'Personal data' means information which uniquely identifies an individual or is capable of doing so. Personal data may be in hard or soft copy (paper/ manual files; electronic records.

1.3 St Elizabeth's needs to process certain personal data about its staff, pupils, students, learners, residents, job applicants and other individuals with whom it has a relationship for various purposes such as, but not limited to the recruitment and payment of staff, the recording of service users health and progress and complying with legal obligations to regulators and funding bodies.

1.4 Under the DPA, St Elizabeth's must ensure that all information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

## 2.0 Responsibilities and enforcement

St Elizabeth's is the 'data controller' under the terms of the legislation, with ultimate responsible for controlling the use and processing of the personal data. If there is evidence of a breach of the DPA, the data controller involved could be subject to enforcement action or prosecution.

The relevant CMT member for the service/ department is responsible for all day-to-day data protection matters, and s/he will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the service/ department.

The Director of Finance is responsible for ensuring that St Elizabeth's notification is kept accurate. Details of the notification can be found on the Office of the Information Commissioner's website (www.informationcommissioner.gov.uk).

This policy applies to all staff, including any processing personal data 'off-site', e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data. each CMT members is responsible for ensuring all staff are trained in data security procedures on a regular basis so they know what is expected of them and the sanctions that apply in event of breach.

Compliance with the legislation is the personal responsibility of all individuals who process personal information. Any breach of this policy, or of the Act itself will be considered an offence and the disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with St Elizabeth's and who have access to personal information, will be expected to read and comply with this policy. It is expected that services/departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

Individuals who provide personal data to St Elizabeth's are responsible for ensuring that the information is accurate and up to date.

**3.0 Data Protection Principles**

3.1 The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

3.2 In order to comply with its obligations, St Elizabeth's undertakes to:

*1 – Process personal data fairly and lawfully*

St Elizabeth's will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

If it is possible to satisfy business' needs without retaining information in a form that can identify people, St Elizabeth's will do so.

*2 – Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose*

St Elizabeth's will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

*3 – Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed*

St Elizabeth's will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind.

*4 – Keep personal data accurate and, where necessary, up to date*

St Elizabeth's will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the organisation if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the organisation to ensure that any notification regarding the change is noted and acted on.

*5 – Only keep personal data for as long as is necessary*

St Elizabeth's undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means St Elizabeth's will undertake a regular review of the information held and implement a weeding process when data subjects leave the organisation.

St Elizabeth's will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion; shredding and disposal of hard copy files as confidential waste).

*6 – Process personal data in accordance with the rights of the data subject under the legislation*

Individuals have various rights under the legislation including:

- a right to be told the nature of the information St Elizabeth's holds and any parties to whom this may be disclosed
- a right to prevent processing likely to cause damage or distress
- a right to prevent processing for purposes of direct marketing
- a right to be informed about the mechanics of any automated decision taking process that will significantly affect them
- a right not to have significant decisions that will affect them taken solely by automated process
- a right to sue for compensation if they suffer damage by any contravention of legislation
- a right to take action to rectify, block, erase, or destroy inaccurate data
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened

St Elizabeth's will only process personal data in accordance with individuals' rights.

*7 – Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data*

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

St Elizabeth's will ensure that all personal data is accessible only to those who have a valid reason for using it. St Elizabeth's will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access)
- keeping all personal data in a lockable room with key-controlled access
- password protecting personal data held electronically on a secure server
- archiving personal data on disks which are then kept securely (lockable cabinet)
- placing any computer screens, etc that show personal data so that they are not be visible except to authorised staff
- ensuring that computer screens are not left unattended without a password protected screen-saver being used.

In addition, St Elizabeth's will put in place appropriate measures for the deletion of personal data, manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work.

*8 – Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data*

St Elizabeth's will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet, as transfer of data can include placing data on a website that can be accessed from outside the EEA, so St Elizabeth's will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If St Elizabeth's collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

**4.0 Consent as a basis for processing**

4.1 Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

4.2 Consent* is especially important when processing any sensitive data, as defined by the legislation as : racial or ethnic origin, political opinions, religious beliefs or similar, trade union membership, physical or mental health, sexual life, commission of, or alleged commission of, any offence (and any court proceedings or sentencing).

* although there are some exceptions to this, for example, where it is necessary in order to comply with a legal obligation in connection with an individual's employment.

St Elizabeth's understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

4.3 St Elizabeth's will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

4.4 St Elizabeth's will ensure that if the individual does not give his/ her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

4.5 Collecting information about children and vulnerable people who may find it difficult to understand how their information is used. In order to process data fairly, it is recognised to be important to try to assess the level of understanding of (potential) data subjects in order to avoid exploiting any lack of understanding on their part.

For example, it is recognised good practice to seek parental consent if the collection or use of information about a child is likely to result in:

- disclosure of a child's name and address to a third party, for example as part of the terms and conditions of a competition entry;
- use of a child's contact details for marketing purposes;
- publication of a child's image on a website that anyone can see;
- making a child's contact details publicly available; or
- the collection of personal data about third parties, for example where a child is asked to provide information about his or her family members or friends.

**5.0 Subject Access Rights (SARs)**

5.1 Individuals have a right to access any personal data relating to them which are held by the organisation. Any individual wishing to exercise this right should apply in writing to the relevant CMT member with overall responsibility for that service or, in the case of staff or job applicants, to the Director of HR.

5.2 Any member of staff receiving a SAR should forward this to the relevant member of CMT.

5.3 St Elizabeth's reserves the right to charge a fee for data subject access requests (currently £10).

5.4 Under the terms of the legislation, any such requests must be complied with within 40 days.

**6.0 Disclosure of Data**

6.1 St Elizabeth's undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies, and in some circumstances, the police.

6.2 Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure
- the disclosure has been notified to the Office of the Information Commissioner and is in the legitimate interests of the organisation
- the organisation is legally obliged to disclose the information the disclosure is required for the performance of a contract

6.3 There are other instances when the legislation permits disclosure without the consent of the individual. For detailed guidance on disclosures see the DPA Code of Practice..

6.4 It is the policy of St Elizabeth's to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the organisation may be accessed by someone other than the recipient for system management and security purposes.

6.5 In no circumstances will St Elizabeth's sell any of its databases to a third party.

**7.0 Review and updating**

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the DPA and other relevant legislation.

**8.0 Further information**

- http://www.nationalarchives.gov.uk/information-management/projects-and-work/retention-disposal-schedules.htm
- http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx
- http://www.informationcommissioner.gov.uk. This includes sector guides, e.g. charities, employment, health and education.