DATA PROTECTION POLICY

DATE CREATED	2018	**DATE OF NEXT REVIEW**	September 2025
DATE APPROVED	September 2024		
POLICY OWNER(S)	Data Protection Officer		
DESIGNATION	Centre wide		
APPROVED BY	Board of Trustees		

Purpose of policy	To set out St Elizabeth's policy to ensure compliance with Data Protection legislation
Intended audience	All staff
Links to other policies	Privacy Notices; Business Continuity and Emergency Planning Policy; Bring your Own Device Policy, Internet Filtering Policy, Information Security Policy, Communications, Email and Internet Policy, Fundraising Policy.
Reviewed	2021 2023

St Elizabeth's Centre

Data Protection Policy

1. Background

1.1. St Elizabeth's Centre ("the Charity") is committed to the highest level of data protection. The Charity will follow the relevant Law taking into account any relevant guidance.

1.2. "**Law**" means the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, the Data Protection (Charges and Information) Regulations 2018 and the Privacy and Electronic Communications Regulations 2003, as amended from time to time.

1.3. "**Guidance**" means any guidance issued by the Information Commissioner's Office (ICO).

2. Scope

2.1. This policy applies to any information which is 'personal data' as defined in article 4 of the GDPR; broadly this means information about a natural person who can be identified directly or indirectly. In any case where it is not clear whether the information in question is personal data, a cautious approach will be adopted and such information will be treated as personal data.

3. Definitions

3.1. "**Data controller**" means the natural or legal person or organization which, alone or jointly with others, determines the purposes and means of the processing personal data. For the purposes of this Policy the Charity is the data controller of all personal data relating to data subjects used in the business for our commercial and charitable purposes.

3.2. "**Data processor**" means a natural or legal person or organization which processes personal data on behalf of a data controller

3.3. "**Personal data**" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

3.4. "**Special Category Data**" is the most sensitive personal data and includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data for the purpose of

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. "ICO" is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

4. Organisational Responsibilities

4.1. The Charity has the ultimate responsibility for compliance with data protection law. In practice, this means that it is the responsibility of the Trustees of the Charity. The Trustees may delegate tasks but not ultimate responsibility.

4.2. The Trustees have delegated the responsibility for implementing this policy and monitoring compliance to the Data Protection Officer and Executive Team.

4.3. We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Charity.

4.4. The Trustees and staff working together ensure that the data protection principles (set out below) are complied with and that the Charity is able to demonstrate this.

4.5. The Data Protection Officer is responsible for overseeing this policy and developing data-related policies and guidelines.

4.6. Please contact the Data Protection Officer with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

4.7. The Data Protection Officer must be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and/or process personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing.

4.8. The Data Protection Officer's contact details are set out below:

- Data Protection Officer: Mike Bibby
- Email: DPO@stelizabeths.org.uk
- Telephone: 01279 844 361

5. Data Protection Principles

5.1. The Charity will comply with the principles of data protection which are set out below.

5.2. All personal data shall be:

a) processed lawfully, fairly and in a transparent manner;

b) collected for specific explicit and legitimate purposes and shall not be further processed in a manner which is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purpose;

d) accurate and where necessary, kept up to date;

e) kept in a form which permits identification of individuals for no longer than necessary for the purpose; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.3. The Charity will make sure that it is able to demonstrate compliance with these principles.

6. Staff Responsibilities

6.1. A member of staff's job description will set out any specific data protection responsibilities which they have. All staff including volunteers are expected to ensure compliance with the

law by following all relevant policies and procedures and in particular shall follow these rules:

a) Make sure that any personal data held is accurate and up to date.

b) Follow the Charity's Records Retention Policy and do not keep personal data longer than necessary.

c) Make sure you store personal data carefully in accordance with the procedures in your team. Do not leave it unsecured, whether at work, when working at home or when travelling.

d) Be careful when you send personal data outside St Elizabeth's. Make sure that you are allowed to do so and protect it during transit, following the IT policies (Information Security Policy, Communications, Email and internet Security Policy and Bring your Own Device (BYOD) Policy), all of which may be found on the intranet) at all times.

e) Inside the Charity, only share personal data on a 'need to know' basis.

f) Respect the rights of individuals by actioning any individual requests by referring them as required in this policy.

g) Be very careful about making a new collection of personal data or using existing data for a new purpose. Proper consideration must be given to this and the Data Protection Officer must be consulted.

7. The Personal Data which the Charity holds

7.1. The Charity holds personal data about a number of different categories of individuals. These are set out below together with an indication of the type of personal data held. The Charity will not process personal data unless it is lawful to do so. Apart from some exemptions laid down by law, any processing of personal data can only take place if certain conditions are met. All processing must have a lawful basis which is set out in article 6 of the UK GDPR (General Data Protection Regulation) and in the case of Special Category Data a condition in article 9 of the UK GDPR must also be met. Individuals are provided with a privacy notice explaining the conditions which apply.

7.2. The available article 6 bases are:

a) **Consent:** the individual has given clear consent for The Charity to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract The Charity has with the individual, or because they have asked us to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for The Charity to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for The Charity legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

7.3. Whenever the processing of personal data is based on legitimate interests, those legitimate interests must be fully assessed using the legitimate interest assessment template provided by the ICO. The available article 9 bases are:

a) Explicit consent

b) Employment, social security and social protection (if authorised by law)

c) Vital interests

d) Not-for-profit bodies

e) Made public by the data subject

f) Legal claims or judicial acts

g) Reasons of substantial public interest (with a basis in law)

h) Health or social care (with a basis in law)

i) Public health (with a basis in law)

j) Archiving, research and statistics (with a basis in law)

7.4. Whenever personal data is processed on the basis of article 9 (b), (g) or (h) an appropriate policy document based on the ICO template must be in place.

7.5. The Charity holds personal data as follows:

<u>Those who work for St Elizabeth's:</u>

- Employees (including bank staff)
- Agency Staff
- Volunteers

We hold a range of personal data about the above people. The personal data will include information which is Special Category Data (sensitive information) in particular information relating to health. We only collect this where it is needed in connection with the role at The Charity and where we have established a legal justification (called a legal basis) for having this information. All employees (including bank staff), agency staff and volunteers are provided with a privacy notice which gives further details of the information we have about them and why we have it.

<u>Service Users:</u>

- Residents in the Children's Home
- Supported Living plus Windhill

- Pupils attending the School
- Students attending the College
- Those attending Day Opportunities

We hold a range of personal data about the above people. The personal data will include a large amount of information which is Special Category Data (sensitive information), in particular information relating to health. We only collect this where it is needed in connection with the services which we provide and where we have established a legal justification (called a legal basis) for having this information. All service users (or their parent, guardian(s) or representative(s)) are provided with a privacy notice which gives further details of the information we have about them and why we have it.

Other contacts:

- Contractors
- Employees of other organisations with whom we come into contact in the course of running The Charity
- Parents / guardians / representatives of service users
- Emergency contacts for service users / staff

The personal data which we have about the above contacts is ordinary contact information. For contractors and employees of other organisations, this will normally be business contact details such as name, telephone number and business email address. For parents / guardians / representatives and emergency contacts, we also collect personal contact details such as home phone number and address, and the relationship to the service user. Further details are in the relevant privacy notices provided to individuals.

8. Disclosure of Personal Data

8.1. No disclosure of personal data will be made unless the disclosure is permitted by law. Apart from some exemptions laid down by law, any processing of personal data including disclosure of it can only be done if certain conditions are met. All processing must have a lawful basis which is set out in article 6 of the UK GDPR (General Data Protection Regulation) and in the case of Special Category Data a condition in article 9 of the UK GDPR must also be met. See section 7 for an explanation of articles 6 and 9. Individuals are provided with a privacy notice explaining the conditions which apply.

8.2. **Sharing personal data internally**

Personal data should only be shared with other members of staff or teams on a ‘need to know basis’ This is particularly important where the information is Special Category Data (sensitive information).

8.3. **Sharing personal data outside the Charity**

Data must not be shared routinely unless it is covered by existing documented data sharing arrangements. When relying on such an arrangement care should be taken to make sure that the sharing is within the agreed terms i.e. it is personal data of the sort covered by the arrangement and it is being shared for the purpose set out in the arrangement. If no sharing arrangement is in place or if the existing arrangement does not cover the sharing, then the Data Protection Officer must be consulted. It is important that a decision to share personal data is carefully considered and documented, even if it a disclosure that will only be required very rarely.

In line with the principle of accountability, the Charity must check that they are being responsible in disclosing personal data to another organisation. All reasonable efforts should be made to ensure that the organisation to which the personal data is to be disclosed meets a good standard of compliance with data protection law.

Before any personal data is shared, the potential need for a Data Protection Impact Assessment (DPIA) to be carried out will be assessed having regard to the ICO guidance and checklists. A DPIA must be carried out in any case where there is a high risk to individuals. In a case where high risk cannot immediately be ruled out a DPIA should be carried out as this is the best way to assess the level of risk.

9. Data Processing Arrangements

9.1. The Charity uses a number of data processors. A data processor processes personal data under the instructions of the Charity. Where an individual's personal data is processed by a data processor this is made clear to them in the privacy notice provided to them. There must by law be a written data processing agreement in place for every data processing arrangement and no data should be processed without such an agreement in place. If a member of staff wishes to use a new processor, then the Data Protection Officer must be consulted before any personal data is disclosed to the processor.

9.2. Before engaging any processor, the Charity will carry out a full due diligence process to check that the processor can provide sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights.

10. New Collection of use of Personal Data

10.1. If a member of staff intends to collect additional personal data or to deploy existing personal data for a new purpose, then they must consult with both their Head of Service and the Data Protection Officer. A data protection impact assessment may need to be carried out to determine whether the new collection or use can go ahead and, if it can, there may be a need to update documentation such as the central record of processing activities (ROPA) or privacy notices.

11. Retention Policy

11.1. The Charity only retains personal data for as long as it needs it. For further details, please see the Records Retention Policy.

12. Individual Rights

12.1. The individuals whose personal data is processed by the Charity have individual rights which are set out below:

a) Right of access

Individuals have the right to ask for a copy of the personal information about them which the Charity holds and to be informed about how it is processed. More information about this right can be found here:

https://ico.org.uk/your-data-matters/your-right-of-access/

b) Right of rectification

Individuals have the right to rectification. This means that they can ask the Charity to correct the personal information it has about them. More information can be found here:

https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected/

c) Right of Erasure

Individuals have the right to erasure also often referred to as the 'right to be forgotten'. This is the right to have their personal information deleted. More information can be found here:

https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/

d) Right to object to processing

Individuals have the right to object to what the Charity does with their personal information. More information can be found here:

https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-yourdata/

e) Right to portability

Individuals have the right to transfer personal data from one organisation to another but this only applies in certain circumstances. More information can be found here:

https://ico.org.uk/your-data-matters/your-right-to-data-portability/

f) Right to withdraw consent

Where the Charity processes personal data on the basis of consent that consent can be withdrawn at any time. More information can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-thegeneral-data-protection-regulation-gdpr/consent/how-should-we-obtainrecord-and-manage-consent/#how6

12.2. Individuals can exercise their rights by contacting the Data Protection Officer. The Charity will normally be under an obligation to respond to the individual within one month, although the deadline may be extended by up to a further two months, where necessary,

taking into account the complexity and number of requests. Individuals should note that the above rights are not absolute and there will be circumstances where they do not apply.

12.3. There is no charge for individual rights requests except where the requests are manifestly unfounded or excessive in which case the Charity may either:

a) charge a reasonable fee to cover administrative costs, or

b) refuse to act on the request(s).

13. Handling of Individual Rights Requests

13.1. Receiving a request and verifying identity

When someone contacts the Charity to make an individual rights request, the request shall be referred to the Data Protection Officer immediately or in their absence to the CEO. If a request is made verbally then the staff member who receives the request should make a written note of what the person is asking so that the Data Protection Officer can check this with the individual.

The Data Protection Officer will identify which individual rights apply to the request made by the individual referring to the ICO guidance and seeking legal advice if needed.

The Data Protection Officer will confirm the identity of the person making the request before disclosing any personal data to them. [Formal identification is not necessary where the Data Protection Officer is already certain of the identity of the person and that it is that person who has approached the Charity and made the request. An example of where the Data Protection Officer can be certain would be where an individual has made a request using an email address they always use and the Charity is able to check with them that they did send the email. The issue of identification of the requester should always be approached with caution because of the risk of fraud. In any case where the identity of the individual is not certain, the identity must be verified using reliable documents such as a passport or photo card driving licence. A full list of acceptable documentation is listed below:

Proof of Name	Proof of Address
Current signed passport	Utility bill (gas, electric, satellite television, landline phone bill) issued within the last three months
Original birth certificate (UK birth certificate issued within 12 months of the date of birth in full form including those issued by UK authorities overseas such as Embassies High Commissions and HM Forces)	Local authority council tax bill for the current council tax year
EEA member state identity card (which can also be used as evidence of address	Current UK driving licence (but only if not used for the name evidence)

if it carries this)	
Current UK or EEA photo card driving licence	Bank, Building Society or Credit Union statement or passbook dated within the last three months
Full old-style driving licence	Original mortgage statement from a recognised lender issued for the last full year
Photographic registration cards for self-employed individuals in the construction industry -CIS4	Solicitors letter within the last three months confirming recent house purchase or land registry confirmation of address
Benefit book or original notification letter from Benefits Agency	Council or housing association rent card or tenancy agreement for the current year
Firearms or shotgun certificate	Benefit book or original notification letter from Benefits Agency (but not if used as proof of name)
Residence permit issued by the Home Office to EEA nationals on sight of own country passport	HMRC self-assessment letters or tax demand dated within the current financial year
National identity card bearing a photograph of the applicant	Electoral Register entry or NHS Medical card or letter of confirmation from GP's practice of registration with the surgery

13.2. **Requests made by someone on behalf of someone else**

Individual requests made by someone other than the data subject (the person the personal data relates to) should be approached with caution. Personal data should not be released unless it is clear that the person making the request has the authority to act on behalf of the person the personal data is about. For example, if a solicitor makes a request on behalf of their client then it will be necessary to ask for the signed authority of their client.

Children can make their own requests if they have capacity and understanding to do so. The age at which they have sufficient capacity and understanding will vary and be affected by any special educational needs they have which would affect their level of understanding. The capacity of a child should be assessed on an individual basis. If a child has capacity, then they should make their own request but if a parent, guardian or representative makes it for them then it is most straightforward if the child confirms that they authorise their parent, guardian or representative to make the request for them. This does not mean that the consent of a child with capacity will always be required for information about them to be given to their parent, guardian or representative, but where a formal individual rights request is received, obtaining the consent of the child will make the request more straightforward to deal with. The ICO guidance recommends this approach.

For adults without capacity, the Charity should check that anyone making requests on their behalf is authorised to do so.

All individual rights requests will be handled in accordance with the law and the Data Protection Officer will take into account the ICO guidance and follow it unless there is a very good reason not to do so. The ICO Guidance can be found here:

Right of access | ICO

14. Personal Data Breach

14.1. Personal Data Breach is defined in the GDPR as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. The following is a non-exhaustive list of events which will be a personal data breach if personal data is affected:

a) loss or theft of data or equipment on which personal data is stored, for example loss of a laptop or a paper file (this includes accidental loss);

b) inappropriate access controls allowing unauthorised use of personal data;

c) equipment failure;

d) human error (for example sending an email or SMS to the wrong recipient);

e) unforeseen circumstances such as a fire or flood; or

f) hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

14.2. When an event occurs, which is or may be a Personal Data Breach the Breach Management Procedure will be implemented.

14.3. **Procedure for handling actual or potential personal data breaches**

The Director of HR, Director of Children Services, Finance Director, Director of Learning and Director of Wellbeing (each a Head of Service) have responsibility for breach notification within their respective areas. They are each responsible for ensuring breach notification processes are adhered to by all staff within their respective service area and are the designated point of contact for personal data breaches for each respective service.

In the absence of the Head of Service, please contact the Data Protection Officer.

14.4. **Reporting a personal data breach internally**

If any member of staff knows or suspects a personal data breach has occurred, they should immediately report it to the Head of Service using the data breach report form (which can be found below at the Appendix or obtained from the Head of Service or the Data Protection Officer and is available on the intranet); and email the completed form to the Head of Service and the Data Protection Officer.

Where appropriate, you should liaise with your line manager about completion of the data breach report form. Breach reporting is encouraged throughout the Charity and staff are

expected to seek advice if they are unsure as to whether the breach should be reported and / or could result in a risk to the rights and freedom of individuals. You can seek advice from the relevant Head of Service or the Data Protection Officer.

Once reported, you should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators or investigate further. The Head of Service will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the Data Protection Officer.

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the Head of Service or the Data Protection Officer. This can help capture risks as they emerge, protect the Charity from personal data breaches and keep our processes up to date and effective.

14.5. **Managing and recording a breach**

On being notified of a suspected personal data breach, the Head of Service will notify the Data Protection Officer. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

a) where possible, contain the data breach;

b) as far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;

c) assess and record the breach in the Charity's data breach register;

d) where relevant, notify the ICO;

e) where relevant, notify data subjects affected by the breach;

f) where relevant, notify other appropriate parties to the breach;

g) take steps to prevent future breaches.

14.6. **Reporting the breach externally**

The Charity must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

a) potential or actual discrimination;

b) potential or actual financial loss;

c) potential or actual loss of confidentiality;

d) risk to physical safety or reputation;

e) exposure to identity theft (for example through the release of non-public identifiers such as passport details); or

f) the exposure of the private aspect of a person's life becoming known by others. If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individual(s) must also be notified directly.

14.7. **Notifying the ICO**

The Head of Service or Data Protection Officer will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the Charity is unsure whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO. The Charity may be fined by the ICO if the breach is reported after the 72- hour point without very good reasons for the delay.

14.8. **Notifying affected individuals**

Where the data breach is likely to result in a high risk to the rights and freedoms of individuals, the Head of Service will notify the affected individuals without undue delay of the breach and of the name and contact details of the Data Protection Officer and ICO, the likely consequences of the data breach and the measures the Charity has taken or intends to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Head of Service will cooperate with and seek guidance from the Data Protection Officer, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Charity will consider alternative means to make those affected aware (for example by making a statement on the Charity's website).

14.9. **Notifying other authorities**

The Charity will need to consider whether other parties need to be notified of the breach. For example:

a) Insurers;

b) Parents / guardian(s) / representative(s);

c) Third parties (for example when they are also affected by the breach);

d) Local authority; or

e) The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

14.10. **Assessing the breach**

Once initial reporting procedures have been carried out, the Charity will carry out all necessary investigations into the breach.

The Charity will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the Charity will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and / or data subjects as set out above). These factors include

a) what type of data is involved and how sensitive it is;

b) the volume of data affected;

c) who is affected by the breach (i.e. the categories and number of people involved);

d) the likely consequences of the breach on affected individuals following containment and whether further issues are likely to materialise;

e) are there any protections in place to secure the data (for example, encryption, password protection, pseudonymised data);

f) what has happened to the data;

g) what could the data tell a third party about the individual;

h) what are the likely consequences of the personal data breach on the Charity; and

i) any other wider consequences which may be applicable.

14.11. **Completing the Personal Data Breach Log**

Following a breach, the Data Protection Officer will log the breach. This record must comprise the facts relating to the personal data breach, its effects and remedial action taken.

14.12. **Preventing Future Breaches**

Once the data breach has been dealt with, the Charity will consider its security processes, with the aim of preventing further breaches. In order to do this, we will:

a) establish what security measures were in place when the breach occurred;

b) assess whether technical or organisational measures can be implemented to prevent the breach happening again;

c) consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;

d) consider whether it is necessary to conduct a data protection impact assessment;

e) consider whether further audits or data protection steps need to be taken;

f) to update the data breach register;

g) to debrief the Executive Team and Audit and Risk Committee and Trustees, following the investigation.

15. Complaints from Individuals

15.1. If at any time you have a complaint about what we do with your personal data, then you can complain to the Charity. The data protection complaints procedure is set out below.

15.2. **The Charity's Data Protection Complaints Process**

On receiving a data protection complaint, the Data Protection Officer will acknowledge it within 10 working days and determine whether or not the complainant is seeking to exercise any of his or her data protection rights, seeking clarity from the complainant as necessary. Sometimes a complaint may in fact be an attempt to exercise an individual data protection right such as 'the right to object'. In other cases, it may be a general complaint about data protection policies and practices with no exercise of individual rights. Sometimes, there may be elements of both.

Data protection complaints may on occasion form part of a complaint about another issue or issues which is being handled under the Charity's general Complaints policy. Where this is the case, the data protection matter will be determined under this data protection complaints policy and referred back to the person handling the main complaint, so that the outcome can be included in the response to the individual's main complaint. The only exception to this will be where there is a relevant statutory deadline which means an earlier response is required (see individual rights below).

15.3. **Individual Rights**

The GDPR provides the following rights for individuals:

a) The right to be informed

b) The right of access

c) The right to rectification

d) The right to erasure

e) The right to restrict processing

f) The right to data portability

g) The right to object

h) Rights in relation to automated decision making and profiling.

Although not usually listed as a separate data protection right, individuals do also have the right to withdraw any consent which they have previously given.

There is more information about individual rights above and in the privacy notices provided to individuals. These rights are not absolute and can be refused in certain circumstances.

Where an individual right or rights is/are being exercised, the Charity will seek to respond within statutory timescales (usually one month, although these may in certain circumstances be extended).

15.4. **How to make a data protection complaint or exercise an individual right**

We would prefer that complaints are made in writing where possible. However, individual data protection rights may be exercised verbally. In the case of verbal requests, we will confirm our understanding of the request in writing. Please make any complaint to:

- Data Protection Officer
- Email: DPO@stelizabeths.org.uk
- Telephone: 01279 844 361

15.5. **Complaints to the ICO**

Alternatively, you can complain directly to the Information Commissioner's Office, although the Information Commissioner's Office will usually expect you to have used the Charity's complaints process before complaining to the Information Commissioner's Office:

Information Commissioner's Office Wycliffe House

Water Lane Wilmslow Cheshire SK9 5AF

Telephone: 0303 123 1113

16. Policy Review

16.1. This policy will be reviewed routinely every two years but may be reviewed more frequently if required in response to events (such as personal data breaches, complaints or changes to the law) or recommendations from the Data Protection Officer.

APPENDIX – St Elizabeth's

Personal Data Breach Notification Form (for internal use)

This form, to be prepared in conjunction with the St Elizabeth's Data Breach Policy, is for staff / members / volunteers to report a Personal Data Breach at St Elizabeth's. Please complete the form and return it to the relevant Head of Service and the DPO, DPO@stelizabeths.org.uk immediately.

Name of the person reporting incident	
Phone number	
Email address	
Role	
Department	

Please fill out the boxes below if different from above.

Name of person(s) responsible for the breach	
Role	
Department	

Please fill out **all** the fields below.

What date(s) did the breach occur?	
What date was the breach discovered?	
What date was the breach reported?	
Briefly describe the breach • How did it occur? • Media coverage? • Police involvement (crime number if applicable) • Systems affected (GO / Payroll / Finance)	

Has any personal data been disclosed? Please give details. Examples include names, contact details, and health information.	
How many people have been affected?	
Did it contain children's data? In this instance, children are those under 18.	
Did it contain Special Category Data or data relating to criminal convictions and/or offences? Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data.	
What steps have you taken to minimize the effect/risk? Please give details.	
Have the individual(s) parent(s) / Guardian(s) / representative(s) been informed, if applicable? If they haven't please contact is for guidance.	