Privacy Notice for Learners at St Elizabeth's College

DATE CREATED		**REVIEWED** **DATE OF NEXT REVIEW**	October 2024 November 2025
POLICY OWNER(S)	Director of Learning		
DESIGNATION	College		

Purpose of policy	The purpose of this notice is to explain how St Elizabeth's Centre uses your personal data.
Intended audience	Learners, Parents, Guardians
Links to other policies	

This notice is addressed to the learner but is provided to the parent or guardian or appointed person of the learner as our learners do not have capacity to understand this notice, or do not have capacity to understand it without the assistance of their parent, guardian or appointed person.

St Elizabeth's College is run by the charity called St Elizabeth's Centre. This notice explains how St Elizabeth's Centre uses your personal data. Personal data means information about you or which relates to you in some way.

Our Contact details
St Elizabeth's Centre
South End
Much Hadham
Hertfordshire
SG10 6EW
Tel: 01279 843451

St Elizabeth's Centre is the Controller for the purposes of data protection law.

The Data Protection Compliance Officer for St Elizabeth's Centre is Mike Bibby.

The Type of Personal Information we collect about you

- Your name
- personal identifiers and contacts (such as name, date of birth unique pupil number, contact details and address)
- characteristics (such as free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs
- medical information (such as mental capacity assessments, seizures and interventions, doctors' information, child health, dental health, allergies, medication and dietary requirements, personal care)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (how well you are doing at college)
- information about your behaviour

Why we collect and use learner information

We collect and use pupil information, for the following purposes:

a) to support learners' learning
b) to monitor and report on learner attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep learners safe (food allergies, or emergency contact details)
f) to comply with legal requirements
g) to meet standards of good practice including Ofsted requirements

Legal Basis

Under the General Data Protection Regulation (GDPR), article 6, the lawful bases we rely on for processing pupil information are:

Legal obligation

We use this when we have to use your personal data to comply with a legal obligation. For example, we are required by law to collect some information about pupils.

Legitimate Interests

This is used when we have established that we have a legitimate interest in using your personal data and we have balanced our interest against your interests. We use this for some photographs and videos which are for use in College or by families (see photograph policy for further details).

Consent

This is used when we ask you or your parent, guardian, or other appointed person for consent.

Public interest

We use this when we are using your personal data to provide disability support or help keep you safe.

Some information we collect about you is special category data. This covers the information we have about your health. We use substantial public interest for this. The substantial public interest is:

1. support for individuals with a particular disability or medical condition
2. safeguarding of children and of individuals at risk

Collecting learner information

We collect information about you from your parents before you start at the College. We may also get some information about you from your last school or from the Local Authority. Once you are at the College we may record other information about you because you are a learner so that we can look after you, help you to learn and record your progress.

Most of the information we ask for is necessary. A learner may not be able to start at the College if it is not provided. If there is a choice about whether to give us information or not, then we will tell you that it is optional.

Storing learner data

We hold learner data securely for the set amount of time shown in our data retention policy. Normally this will be until you reach age 25. Our data retention policy gives more information about how long we keep information about you.

How we store your personal data

Your information is stored securely on both local servers and cloud based systems. All access is restricted by username and password authentication.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact:
DPO@stelizabeths.org.uk
You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection Regulations.

If you have a concern about the way we are collecting or using your personal data or wish to exercise any of the rights above, we request that you raise your concern with us in the first instance at: DPO@stelizabeths.org.uk

Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

How we keep data up to date

All data that is used within the organisation, is saved on to systems and kept up to date via 'Pegasus'.

How we dispose of confidential waste

St Elizabeth's Centre uses WEE recycling to dispose of redundant IT equipment.
In addition to this, whilst no personal data is saved to local PCs and Laptops, secure data destruction is performed. This ensures that all confidential information is destroyed.

Requirements for sharing or transferring data outside of the organisation

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 Compliance 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, St Elizabeth's Centre 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.

Procedures in place if personal data is lost or stolen

MDM policy in place. No unauthorised software can be installed. If a device is lost or stolen, it will be remotely wiped.
The Registered Manager of the Children's Home, Head Teacher, Head of College and Head of the Adult Services have responsibility for breach notification within their respective areas (Head of Service). 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 Compliance Officer.

- **Managing and recording a breach** On being notified of a suspected personal data breach, the Head of Service will notify the Data Protection Compliance 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 St Elizabeth's Centre'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.

- **Reporting the breach externally** St Elizabeth's Centre 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.

- **Notifying the ICO** The Head of Service or Data Protection Compliance 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 St Elizabeth's Centre is unsure of 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. St Elizabeth's Centre may be fined by the ICO if the breach is reported after the 72-hour point without very good reasons for the delay.

- **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 including the name and contact details of the Data Protection Compliance Officer and ICO, the likely consequences of the data breach and the measures the Charity has taken or intend 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 Compliance 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 St Elizabeth's Centre will consider alternative means to make those affected aware (for example by making a statement on the Charity's website).

- **Notifying other authorities** St Elizabeth's Centre 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); 12 (d) Local authority; or (e) The police (for example if the breach involved theft of equipment or data). This list is non-exhaustive.

- **Assessing the breach** Once initial reporting procedures have been carried out, St Elizabeth's Centre will carry out all necessary investigations into the breach. St Elizabeth's Centre 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, St Elizabeth's Centre 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, pseudonymisation); (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 St Elizabeth's Centre; and (i) any other wider consequences which may be applicable.

- **Completing the Personal Data Breach Log** Following a breach, the Data Protection Compliance Officer will log the breach. This record must comprise the facts relating to the personal data breach, its effects and remedial action taken.

- **Preventing Future Breaches** Once the data breach has been dealt with, St Elizabeth's Centre 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; 13 (f) to update the data breach register; (g) to debrief the Senior Leadership Team, Finance Audit and Risk Committee and Trustees, following the investigation.

What we expect from our staff who work with personal data

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 Centre. 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 St Elizabeth's Centre, only share personal data on a 'need to know' basis. 4 (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 Compliance Officer (Mike Bibby) must be consulted.

The use of security systems, such as computer passwords and firewalls

We store personal information securely within the Centre, for example within hard copy files which are kept securely in locked filing cabinets. It is also held on secure IT systems. Personal information (eg emails, spreadsheets, letters) may also be held on the St Elizabeth's IT system (local servers). Personal information is also stored securely on both local servers and cloud based systems. All access is restricted by username and password authentication.
Where personal information is stored on an externally hosted or managed IT system on behalf of the Centre, the provider is expressly required to confirm compliance with GDPR. No personal data is held outside the EEU.

Who we share learner information with

We routinely share learner information with:

- Local Authorities
- Services for Young People – (formerly Connexions)
- the Department for Education (DfE)
- Education & Skills Funding Agency (ESFA)
- Ofsted
- City and Guilds
- Curriculum Enrichment Activities

Why we regularly share learner information

We do not share information about our learners with anyone without consent unless the law and our policies allow us to do so.

Local Authorities

We share information about your Education Health and Care Plan with the Local Authority because the Local Authority is responsible for maintaining the Plan.

Data is securely transferred to the Local Authority via secure e-mail/Egress.

We also share learner data on safeguarding issues.

Services for Young People

We also pass learner information to our Local Authority and / or provider of Services for Young People as they have responsibilities in relation to the education or training of learners under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can object to any information in addition to their son/daughter's name, address and date of birth being passed to their local authority or provider of youth support services by informing us. This right is transferred to the learner once they reach the age 16 but in practice will continue to be exercised by the parent, guardian or other appointed person where the learner does not have the capacity to make an objection for themselves.

Data is securely transferred to the youth support service via secure e-mail/Egress**.**

Department for Education

The College is routinely required to provide learner data to the Department for Education (or the ESFA which is part of the Department for Education). This will mostly be through the Individual Learner Record (ILR). This data calculates the ESFA funding allocation.

Ofsted

The College is regulated by Ofsted and during the course of an inspection, Ofsted may view information relating to learners. The Education Act 2005 gives Ofsted inspectors the power to inspect and take copies of any records that are relevant.

City and Guilds

As an awarding organisation, City & Guilds require details of individuals that are undertaking accreditation, to enable them to engage with the curriculum. The data is managed through a secure website

Curriculum Enrichment Activities

The College does not provide any personal data to any activity providers, except for Church Farm, to which learners' names are provided.

Use of Processors

We use processors to process some information on our behalf. Processors have a contract with us and must follow our instructions and keep your information secure.

The centre uses on site archiving electronic software package.

Request Your data protection rights

You have the following rights in relation to your personal information:

Right of access

- You have the right to ask for a copy of the personal information which we have about you. You can find out more here: https://ico.org.uk/your-data-matters/your-right-of-access/

Right of rectification

- You have the right to rectification. This means that you can ask us to correct the personal information we have about you. You can find out more here: https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected/

Right of Erasure

- You have the right to erasure also often referred to as the 'right to be forgotten'. This is the right to have your personal information deleted. You can find out more here: https://ico.org.uk/your-data- matters/your-right-to-get-your-data-deleted/

Right to object to processing

- You have the right to object to what we do with your personal information. You can find out more here: https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/

Right to portability

- This right only applies if we are using your personal data and the legal basis for us doing so is either consent or performance of a contract with you as an individual. This means that most of the time it will not be relevant. In certain circumstances, it means that you can ask us to transfer your personal data to another organisation. This only applies where you have provided the personal data to us and we hold it electronically. You can find out more here: https://ico.org.uk/your-data- matters/your-right-to-data-portability/

Right to withdraw your consent

- We do not normally use your personal data on the basis of consent but where we do you may withdraw your consent. In cases where your right to withdraw consent is not relevant, you could use your right to object instead.

You can find out more here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/#how6

To use any of your rights, please contact us by telephoning 01279 843451,

We will normally be under an obligation to respond to you within one month, although we are sometimes permitted to extend the deadline.

Transfers of Personal data

We do not routinely transfer personal data overseas but in the event this was necessary we ensure that we have appropriate safeguards in place.

How to complain

If at any time you have a complaint about what we do with your personal data, then you can complain to us by contacting the Data Protection Compliance Officer for St Elizabeth's Centre:

(dpo@stelizabeths.org.uk

or you can complain directly to the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113