Privacy Notice Policy Statement

DATE CREATED	July 2022	**DATE OF NEXT REVIEW**	July 2023 September 2025
POLICY OWNER(S)	DPO and Head Teacher		
DESIGNATION	School		

Purpose of policy	How we use pupil information
Intended audience	All school staff
Links to other policies	

Privacy Notice- How we use pupil information at St Elizabeth's School

The categories of pupil information that we collect, hold and share include:

- personal information (such as name, unique pupil number and address)
- characteristics (such as ethnicity, language, nationality, country of birth and free
- school meal eligibility)
- attendance information (such as sessions attended, number of absences and absence
- reasons)
- assessment information and related data about attainment and progress
- relevant medical information
- Special Education Needs information
- exclusions
- behavioural information
- personal information about a pupil's parents and/or other relatives (such as name,
- contact details, relationship to child)

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to check for entitlement for pupil's free school meals
- to check for Early Years pupil's entitlement and claim for pupil premium
- to assess the quality of our services
- to comply with the law regarding data sharing
- to share data for statutory inspections and audit purposes

The lawful basis on which we use this information

- We collect and use pupil information under
- The Education Act (various years)
- The Education (Pupil Registration) (England) Regulations
- The School Standards and Framework Act 1998
- The School Admissions Regulations 2012
- Children and Families Act 2014
- The Special Educational Needs and Disability Regulations 2014
- Article 6, and Article 9 (GDPR) – from 25 May 2018 (includes special category data

The DfE process census data under the various Education Acts – further information can be found on their website: https://www.gov.uk/education/data-collection-andcensuses-for-schools

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

- We hold pupil data for varying lengths of time depending on what the information is.
- Pupil personal data until the young person reaches the age of 25 years.
- Pupils safeguarding information until the young person reaches the age of 25 years or longer if deemed necessary.
- RM Integris record of dates of attendance at the School indefinitely.
- Project Search intern's personal data until the age of 25years or until ongoing support ends whichever is the later.

Who we share pupil information with

We routinely share pupil information with:

- Schools, colleges and adult provisions that the pupils attend after leaving us
- our local authority authority (Hertfordshire)
- Individual pupils' local authorities if not Hertfordshire
- the Department for Education (DfE)
- School nursing services (NHS)
- Physiotherapists
- Speech therapists
- Education psychology services
- Education welfare service

- Occupational Therapists
- St Elizabeth's College (secondary pupils only)
- Careers service (secondary pupils only)
- Schools which pupils attend for inclusion

Why we share pupil information

We do not share information about pupils with anyone without consent unless the law and our policies allow us to do so. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/datacollection-and-censuses-for-schools.

Youth support services
Pupils aged 13+

Once the pupils reach the age of 13, we also pass pupil information to the individual pupils local authority. provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds 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 request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16

We will also share certain information about pupils aged 16+ with the individual pupils' local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit the local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-andsupporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received
To contact DfE: https://www.gov.uk/contact-dfe

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:
Mukesh.sharma@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: mukesh.sharma@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

St Elizabeth's Centre use 'Integris', a secure Government package, which is a tool used to feed relevant information into the Department for Education. To allow for this information to be kept up to date, 'Integris' is completed daily.
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 of School, Head of College and Head of the Adult Care 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 (Venetia Phipps) 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.