St. Joseph's Specialist Trust
Amlets Lane, Cranleigh
Surrey GU6 7DH

Website: www.st-josephscranleigh.surrey.sch.uk

GDPR & Data Protection Policy

Christ in our Lives
'No limits ... just possibilities'

***Reviewed**: January 2023*
3 Yearly
STATUTORY POLICY
TRUSTEE POLICY

St Joseph's Specialist Trust

GDPR & DATA PROTECTION POLICY

Contents

Introduction and Purpose of Policy

The policy is applicable to St. Joseph's Specialist Trust which comprises St Joseph's specialist school, college, registered children's home and Springvale and Long Barn, together "St Joseph's".

The purpose of this policy is to provide information about St Joseph's approach to collecting and using personal data in the course of our day-to-day work as well as the rights available to those whose data we hold.

It applies to personal data we collect both as an employer and as an education and care provider, such as that contained within pupil and staff records as well as information we hold on parents, Trustees, Governors, volunteers, visitors and other individuals with whom we interact.

Details of our Data Protection Officer can be found at the end of this policy document and requests for further information or queries relating to this policy can be sent directly to the Data Protection Officer by email to GDPR@st-josephscranleigh.surrey.sch.uk or admin@satswana.com .

The Trustees of St Joseph's have overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Executive Principal and Trustees of St. Joseph's intend to comply fully with the requirements and principles of the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (from May 2018) (now referred to as GDPR). All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Policy Statement

The Executive Principal and Trustees of St. Joseph's are committed to ensuring that personal data is collected and used in a way which is transparent, clearly understood and meets minimum legal requirements and best practice guidance. The Executive Principal and Trustees of St. Joseph's recognise the need for individuals to feel confident that their data will be used only for the purposes that they have been made aware of, and that it is stored securely and for no longer than is necessary. As part of this commitment, we want to ensure that individuals understand the rights available to them if they want to question or raise concerns about the way their data is being processed.

St Joseph's has appointed a Data Protection Officer, Satswana Ltd, whose role is to monitor internal compliance, including with this policy, to inform and advise on data protection obligations and act as a contact point for individuals and the Information Commissioner's Office.

Definitions and Principles

Certain terms are used in this policy which are explained below;-

"processing" means obtaining, recording, holding or destroying the information or data or carrying out any or set of operations on the information or data.

"data subject" means an individual who is the subject of personal data or the person to whom the information relates.

"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media. Data may be held in either paper or electronic records.

Special categories of personal data: this refers to sensitive personal data, which includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

"parent" or family has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

Certain terms are referred to in this policy which are explained below:

"Criminal offence data": this includes data about criminal allegations, proceedings or convictions.

There are certain key **data protection principles** to which St Joseph's must have regard when processing personal data.

These are that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data.

Our Approach to Processing Personal Data

We use privacy notices to inform individuals whose personal data we collect about how we use their information and the legal basis on which we are processing it. If we want to process data for new reasons in the future, we will inform affected individuals first.

We process special categories of personal data and criminal offence data, for example to meet our obligations under employment law. Where we do so, this processing is underpinned by policies on the use of such data.

For some of the data we process we rely on legitimate interests as the legal basis for processing. We do not rely on this basis unless we have first concluded that the rights and freedoms of individuals do not override those interests.

Personal data we hold on individuals is held in secure paper and/or electronic files to which only authorised personnel have access. Information is held for no longer than is deemed necessary, in accordance with our data retention schedules and privacy notices.

If we are planning to process data and this processing is likely to result in a high risk to individuals' interests, we will undertake a Data Protection Impact Assessment (DPIA) to help us identify and minimise the data protection risks.

We always aim to rectify inaccurate or out-of-date information promptly when notified and encourage anyone whose data we hold to inform us when their details have changed.

Data Integrity

St. Joseph's undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs St. Joseph's of a change of circumstances, their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, St. Joseph's will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Trustees for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, St. Joseph's will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered according to our staff and student data retention policies.

Rights of Individuals

If we process your data, you have a number of rights as an individual which are summarised below.

Right to be informed

You have the right to be informed about the collection and use of your data. You must be provided with privacy information about the purposes for which we process your personal data, our retention periods for that personal data and who it will be shared with. Privacy information provided by St Joseph's can be found in our privacy notices which are on the St Joseph's website.

Right of access and Subject Access Requests

You have the right to obtain confirmation from us that your data is being processed and to gain access to your personal data by making a subject access request. Requests for access should be made in writing. You may email your request to GDPR@st-josephscranleigh.surrey.sch.uk or send by post to the St Joseph's address for the attention of the DPO.

In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. We are required to verify your identity before responding which may mean we ask you to provide identification documents.

Parents may request information relating to their child. This will generally require the pupil's consent if the pupil is deemed competent to exercise his/her own rights.

Where a request for subject access is received from a student, St. Joseph's policy is that:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.
- Requests from students who do not appear to understand the nature of the request will be referred to their families.
- Requests from families in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting family.

In most cases we will respond to you within one calendar month of receipt. Please be aware that during closure periods we are unlikely to be able to deal with your request promptly so we ask that, wherever possible, you submit requests during term time.

We do not charge a fee for providing a copy of the information except where we have assessed the request as being manifestly unfounded or excessive or where further copies of the same information are asked for.

If we refuse to respond to a request we will explain why, as well as your right to complain to the Information Commissioner's Office.

Requests for education records: Where a parent has requested access to their child's educational record, this will be provided at no cost within 15 school days of receipt of the written request.

Other individual rights

In addition to the right of access described above, individuals have certain other rights. These are:

- **Right to rectification:** the right to have inaccurate personal data rectified, or completed if it is incomplete.
- **Right to erasure:** the right to have personal data erased (also known as the 'right to be forgotten').

- **Right to restrict processing:** the right to request the restriction or suppression of your personal data in certain circumstances.
- **Right to data portability:** the right in certain circumstances to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.
- **Right to object:** the right to object to processing based on legitimate interests or the performance of a task in the public interest / exercise of official authority; this also covers direct marketing as well as processing for purposes of scientific or historical research and statistics.
- **Rights relating to automated decision making including profiling:** automated individual decision-making refers to making a decision solely by automated means without any human involvement; profiling refers to automated processing of personal data to evaluate certain things about an individual. We do not currently use automated decision making in any of our processing activities

If you want to exercise any of these rights, you should do so by emailing your request to GDPR@st-josephscranleigh.surrey.sch.uk or by post to the St Joseph's address for the attention of the DPO.

International Data Transfers

We do not transfer personal data to countries outside the EEA.

Authorised Disclosures

St. Joseph's will, in general, only disclose data about individuals with their consent. However, there are circumstances under which St. Joseph's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for St. Joseph's to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Student data disclosed to families in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of St. Joseph's.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside St. Joseph's.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within St. Joseph's by administrative staff and teachers will only be made available where the person requesting the information is a professional legitimately working within St. Joseph's who need to know the information in order to do their work.
- St. Joseph's will not disclose anything on student's records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for St Joseph's, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside St Joseph's registered purposes.

Data and Computer Security

St Joseph's undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security

Appropriate building security measures are in place, such as alarms and deadlocks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to St. Joseph's are required to sign in and out, to wear identification badges whilst on site and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

All staff are aware of their Data Protection obligations and receive data protection training. Computer printouts as well as source documents are securely disposed of.

Overall security policy for data is determined by the Executive Principal with the Trustees and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. St. Joseph's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in St. Joseph's should in the first instance be referred to GDPR@st-josephscranleigh.surrey.sch.uk for the attention of the DPO.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Our Approach to Data Security and Breaches

St Joseph's is committed to ensuring that the personal data we hold and process is kept secure at all times and that data protection is considered and integrated into our processing activities. We use a variety of technical and organisational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access. For example, we ensure that:

- only authorised personnel can access, alter or disclose personal data;
- authorised personnel understand the limits of their authority and to whom they should escalate any issues relating to personal data;

- we have appropriate backup systems in place so that, if personal data is accidentally lost, altered or destroyed, it can be recovered;
- access to premises or equipment given to anyone outside St Joseph's (for example, for computer maintenance purposes) is strictly regulated and access to data limited;
- staff receive training to ensure that they receive information on data protection principles and their responsibilities as appropriate to their role, including highlighting the possibility that they may commit a criminal and/or disciplinary offence if they deliberately try to access or disclose information without authority;
- we have proper procedures in place to identify individuals who are requesting personal data before it is given out;
- there are strict guidelines in place on the appropriate use of computers to reduce the risk of the network being compromised;
- we regularly review our physical security measures, such as ease of access to the premises through entrances and internal doors, alarm systems, security lighting and CCTV;
- we have a process in place for the secure disposal of paper waste;
- portable IT equipment is appropriately encrypted so that data contained on such devices is secure;
- confidential paper files are not taken off site unless appropriate security measures are implemented first;
- third parties who process data on our behalf are compliant with data protection law;
- we have an appointed Data Protection Officer in place who monitors and reports on our accountability and governance measures;
- we have a dedicated email address for ease of correspondence regarding all data queries and requests – GDPR@st-josephscranleigh.surrey.sch.uk

Any data breach should be reported to GDPR@st-josephscranleigh.surrey.sch.uk with the words Data Breach in the subject bar. This information will be logged into our breach log and fully investigated by the DPO. The DPO may then decide that it is necessary to report the circumstances to the Information Commissioner within 72 hours of becoming aware that it has occurred.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also inform those concerned directly and without undue delay.

Our Expectations of Staff

We expect all staff working for, or on behalf of St Joseph's, whether employees, casual workers, supply staff, volunteers or consultants, to recognise and adhere to the high standards of data protection we uphold. Everyone has a responsibility for helping to ensure that personal data, whether their own or that of third parties, is accurate, kept up to date and held securely.

Certain members of staff will collect and process data as part of their role. Without exception we expect the following rules to be adhered to:

Members of staff must:

- Only access or process personal data they are authorised to as part of their role and in accordance with the documented purposes for processing (and not for any other purpose);
- Keep personal data confidential and only disclose it to individuals who are authorised to see it (if in any doubt, consulting their line manager or the Data Protection Officer);

- Not remove personal data from its authorised location without permission and, where permission is granted, to ensure that appropriate security measures are in place whilst the data is moved or relocated;
- Not use personal devices such as mobile telephones, cameras, or USB sticks whilst working with our students and must not keep work-related personal data on these or other personal devices.
- Take responsibility for ensuring that personal passwords are strong, are changed regularly and only shared if specifically authorised to do so;
- Adhere to all security measures designed to keep personal data safe from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access;
- Participate in training or briefings and read circulated documents aimed at increasing awareness of data protection legislation and good practice;
- Be aware of data protection issues as part of their day-to-day work, particularly as part of any new projects, and report any concerns relating to personal data (including any potential data breaches) as a matter of urgency to the Data Protection Officer.

These rules are an integral part of St Joseph's data security practices in order to comply with data protection legislation. As such, a breach of these rules is likely to be treated as a disciplinary offence and potentially gross misconduct, in accordance with the disciplinary procedure.

Status of Policy and Review

The content and operation of this policy is reviewed as and when deemed necessary by the Trustees or the Data Protection Officer. The policy is discretionary and does not confer any contractual rights.

Data Protection Officer Contact Details	
Name	**Satswana Ltd**
Email Address	**GDPR@st-josephscranleigh.surrey.sch.uk**
Satswana Telephone Number	***01252 516898***
Satswana Postal Address	***Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH***

Appendix 1

St Joseph's Privacy Notice – (How we use student information)

Appendix 2

St Joseph's Privacy Notice – (How we use workforce information)

Appendix 3

Subject Access Request SAR letter template

Appendix 1
Privacy Notice (How we use student information)
Version and date issued – v2 11.06.2021

At St Joseph's Specialist Trust (St Joseph's) we collect and hold personal information relating to our students, tenants and their parents/carers/guardians. We may also receive information about them from parents, previous schools, local authorities, and/or the Department for Education (DfE). St Joseph's aims to ensure that all data collected about students/ tenants is collected, stored and processed in accordance with the General Data Protection Act (GDPR).

Our Privacy Notice and Data Protection Policy apply to all data, regardless of whether it is in paper or electronic format.

The categories of student/tenant information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as gender, ethnicity, language, nationality, country of birth, special educational needs and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical information (such as doctors contact details, child health, including physical and mental health conditions, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as internal progress assessments and externally set tests)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- Photographs and videos (such as whole school photographs or newsletter items) CCTV images
- Trips and activities (additional information for off-site or on-site activities such as swimming ability)
- Benefit entitlements

Additionally, for parents/carers/guardians, we collect personal information (name, address, contact details) to allow us to communicate with you about your child, young person or adult.

This list is not exhaustive, to access more information about the data that we process please contact GDPR@st-josephscranleigh.surrey.sch.uk to request further information.

Why we collect and use student/tenant information

We collect and use student/tenant information, for the following purposes:

a) to support our student learning and tenant living needs
b) to monitor and report on your child/ young person/ adult's progress
c) to provide appropriate pastoral care
d) to assess the quality of the services that we provide
e) to keep children safe (safeguarding and medical support)
f) to comply with the law regarding data sharing
g) to maintain our own finances, accounts and records
h) to support admissions
i) to monitor attendance and special educational needs

Our legal basis for processing this information under the General Data Protection Regulation (GDPR)

We only collect and use student/ tenants' personal data when the law allows us to. Most commonly, we process it where:

Under Article 6

- We need to comply with a legal obligation (General Data Protection Regulation (EU) 2016/679 (from 25th May 2018) -
  In accordance with the legal basis GDPR Article 6 (1) c) "processing is necessary for compliance with a legal obligation to which the controller is subject"

- We need it to perform an official task in the public interest -
  In accordance with the legal basis GDPR Article 6 (1) e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

However special category data also applies:

Under Article 9

1. "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

2. "Paragraph 1 shall not apply if one of the following applies -

- In accordance with the legal basis GDPR Article 9 (2) a) "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject"

- We need to protect the individual's vital interests (or someone else's interests) – In accordance with the legal basis GDPR Article 9 (2) c) "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent"

Where we have obtained consent to use a student's personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can easily be withdrawn through provision of clear contact details.

Some of the reasons listed above for collecting and using students' personal data overlap and there may be several grounds which justify why we process this data.

How we collect student/tenant information

Student/tenant data is essential for St Joseph's operational use. We collect most of our student/tenant information when they are admitted to St Joseph's through completion of registration forms or Common Transfer File (CTF).

Whilst the majority of student/tenant information we collect from you 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 at the point of collection, whether you are required to provide certain student/tenant information to us or if you have a choice in this. For example, student/tenant photography consent will be requested.

How we store student/tenant data

We hold student/tenant data securely for the set amount of time shown in our data retention schedule.

Who we share student/tenant information with

We routinely share student information with:

- local authorities
- youth support services (students aged 13+)
- the Department for Education (DfE) / ESFA
- schools, colleges and placements that the students attend after leaving us
- the student's family or legal guardians
- our regulators (e.g. Ofsted Care, Ofsted Education, CQC, Regulation 44 Inspector)
- public health authorities and social welfare organisations
- residential trip providers
- formative assessment providers and assessment data management (e.g. BSquared and Caspar)
- Capita SIMS for student database management
- Teachers2parents and Schoolmoney.co.uk (parent online communications and payment systems)
- our school surgery staff, in-house psychiatric and psychology practitioners, and visiting GP
- adult services

This list is not exhaustive, to access more information about the data that we process please contact GDPR@st-josephscranleigh.surrey.sch.uk to request further information

Why we regularly share student/tenant information

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

We share student/tenant data with the Department for Education (DfE), ESFA and other relevant bodies on a statutory basis. This data sharing underpins St Joseph's funding and educational attainment policy and monitoring.

We are required to share information about our students with local authorities and the Department for Education (DfE) under section 3 of the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the National Pupil Database used by the Department for Education go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-andand-supporting-information.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to their 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:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with their 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 your local authority website.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our students with the Department for Education (DfE) either directly or via our local authorities for the purpose of those data collections, under:
Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The Education Act 1996 - Section 537A – states that we provide individual pupil information to the relevant body such as the Department for Education.

Children's Act 1989 – Section 83 – places a duty on the Secretary of State or others to conduct research.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information about how the Government uses your data, the National Pupil Database and data collection requirements placed on us by the DfE (for example via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools or https://www.gov.uk/government/publications/national-pupil-database-user-guide-andsupporting-information

The law allows the DfE to share pupils' personal data with certain third parties, including: schools, local authorities, researchers, organisations connected with promoting the education or wellbeing of children in England, other government departments and agencies, organisations fighting or identifying crime.

For more information about the DfE's NPD data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the DfE has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website:
https://www.gov.uk/government/publications/dfe-external-data-shares

To contact DfE: **https://www.gov.uk/contact-dfe**

Supported Living Tenants

We are required to share some information about tenants with funding providers such as Local Authorities and the CCG in relation to the maintenance of adult placements.

Requesting access to your personal date

Under data protection legislation, parents/legal guardians and students/tenants 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 email GDPR@st-josephscranleigh.surrey.sch.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
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact: Our Data Protection Officer Satswana Ltd by email at GDPR@st-josephscranleigh.surrey.sch.uk for the attention of the DPO.

Appendix 2
Privacy Notice (How we use workforce information)

Version and date issued – v2 11.06.2021

At St Joseph's Specialist Trust ("St Joseph's") we collect and hold personal information relating to our staff, those whom we employ and those who volunteer. We do this to assist in the running of our organisation.
At St Joseph's we take the security of your personal data very seriously. When you apply to join us and throughout your time at St Joseph's you may be asked to provide personal data and consent to the use of personal information.

The categories of information that we process include:

- personal information (such as name, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group, religion)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- details regarding right to work in the UK
- personal identification (such as a copy of your passport)
- safeguarding information and DBS (Data Barring Service) information; a regularly updated enhanced criminal record check for working with adults and children. This can include overseas police checks
- medical information (such as doctors contact details, physical and mental health conditions, dental health, allergies, medication and dietary requirements)
- occupational health referrals and reports
- disability information
- risk assessments
- disciplinary and capability records
- photographs and videos (such as newsletter items)
- CCTV images
- next of kin/preferred contact details (for emergency use)
- bank details for payroll use
- maternity information

This list is not exhaustive, to access the current list of categories of information we process please contact GDPR@st-josephscranleigh.surrey.sch.uk with a request for further information.

Why we collect and use workforce information

We use workforce data to:

a) Visualise the development of a comprehensive workforce and plan deployment
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) keep children safe
e) support the health and wellbeing of our staff

f) provide staff safeguarding and pastoral care
g) comply with the law regarding data sharing
h) maintain our own finances, accounts and records
i) monitor staff attendance
j) to maintain the quality of our provision for all stakeholders

Our legal basis for processing this information under the General Data Protection Regulation (GDPR)

We only collect and use workforce personal data when the law allows us to. This is the lawful basis under the GDPR on which we use this information:

Article 6

1. "Processing shall be lawful only if and to the extent that at least one of the following applies":

Most commonly it is used by St Joseph's for the purposes of:

- Contract –

  (1) b) "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Less commonly we may also lawfully process workforce data held under a special category: **Article 9**

1. "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

2. "Paragraph 1 shall not apply if one of the following applies":

For example, in order for us to –

- Carry out legal obligations as an employer (the data controller) -

  (2) b) "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject"

Collecting workforce information

Staff data is essential for the organisation's operational use. We collect most personal information via completion of forms. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule.

Who we share workforce information with

We routinely share this information with:

- the Department for Education (DfE) / ESFA
- Local Authorities
- The National Office for Statistics
- Others employers where we have express consent (employee reference requests etc.)

Why we share school workforce information

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

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:

We are required to share information about our school employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information about how Government uses your data and to find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-andcensuses-for-schools.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information email GDPR@stjosephscranleigh.surrey.sch.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
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact: Our Data Protection Officer Satswana Ltd by email at GDPR@st-josephscranleigh.surrey.sch.uk

Appendix 3
Subject Access Request (SAR) letter template

Dear Sir / Madam,

Re: Subject Access Request

I am writing to formally make a Subject Access Request for evidence of information that you hold about <name> to which I/we are entitled under the United Kingdom General Data Protection Regulation and the Data Protection Act 2018.

My/Our details can be identified using the following information:

1. Full Name:
2. Address:
3. Email address:
4. Contact number:

Please supply the data about <name> that I/we are entitled to under data protection law including:

1. Confirmation that you are processing <name's> personal data
2. A copy of <name's> personal data
3. The purposes of your processing
4. The categories of personal data concerned
5. The recipients or categories of recipient you disclose <name's> personal data to
6. Your retention period for storing <name's> personal data or, where it is not possible, your criteria for determining how long you will store it
7. Confirmation of the existence of my/our right to request rectification, erasure or restriction or to object to such processing
8. Confirmation of my/our right to lodge a complaint with the ICO
9. Information about the source of the data where it was not obtained directly from me/us
10. The existence of any automated decision-making (including profiling)
11. The safeguards you provide if you transfer my personal data to a third country or international organisation
12. Any and all other information you hold about <name> and how it is used, stored and shared.

I/we look forward to receiving your response to this request for data within one calendar month, per the United Kingdom General Data Protection Regulation and the Data Protection Act 2018. If you do not normally deal with these requests, please pass this letter to your Data Protection Officer, of relevant staff member.

Yours faithfully,

Date Policy Reviewed

Updated	Changes	By	Version
June 2006		Mary Fawcett	v1
October 2009		Mary Fawcett	v1.1
November 2014	Head teacher changed to Principal. Remains in line with Surrey CC model policy	Sue Collins	v1.2
March 2015	To include Long Barn and Springvale	Sue Collins	V1.3
September 2016	Minor typo reference and amend layout	Sue Collins	V1.4
May 2018	Additions and changes in line with GDPR and new Surrey CC model policy	Liz Sanders	V1.5
Sept 2018	Amended to reflect change from St Joseph's Specialist School & College to St Joseph's Specialist Trust	Sue Collins	V2
March 2020	Amendments re Trust and DPO	Lizzie Hurst	V3
March 2021	Revised process and DPO details, added appendices	Lizzie Hurst	V3.1
June 2021	Appendices updated to V2	Lizzie Hurst	V3.2
December 2021	Addition of template SAR letter	Lizzie Hurst	V3.3
January 2023	Minor amendments	Lizzie Hurst	V3.4