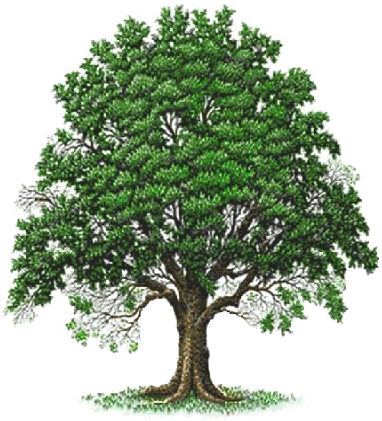
St. Joseph's Specialist School & College
& Supported Living
Amlets Lane, Cranleigh
Surrey GU6 7DH

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

Data Protection Policy



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

Your Life ... Your Way

Reviewed: May 2018
Finance, Personnel & Pay Committee
3 Yearly

STATUTORY POLICY

St Joseph's Specialist School & College

DATA PROTECTION POLICY

Contents

Introduction and Purpose of Policy

The policy is applicable to St. Joseph's Specialist School and College and to Springvale/Long Barn Supported Living; for the purposes of this policy these parties are now referred to as "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, 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

The Governing Body of St Joseph's has 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 Governors of St. Joseph's intend to comply fully with the requirements and principles of the Data Protection Act 1984, the Data Protection Act 1988 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.

General Statement

The Executive Principal and Governors of St. Joseph's is 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 Governors 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 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.

Enquiries

Information about St. Joseph's Data Protection Policy is available from the Director of Business Services. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545745, website www. dataprotection.gov.uk).

Fair Obtaining and Processing

St Joseph's School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal

data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

"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 Governing Body 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 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 must be made in writing (this includes letter, email, fax, social media or through agreed meeting minute taking). You may email your request to GDPR@st-josephscranleigh.surrey.sch.uk or by post to the St Joseph's School and College address. 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 school and college address.

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

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are aware of their Data Protection obligations. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Executive Principal with the Governing Body 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.

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;
- induction training has been introduced to ensure that staff 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;
- 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, however severe, should be reported to GDPR@st-josephscranleigh.surrey.sch.uk. This information will be logged into our breach log and fully investigated by the Data Protection Officer (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 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.

Data Protection Officer Contact Details	
Name	**Sue Collins**
Email Address	**GDPR@st-josephscranleigh.surrey.sch.uk**
St Joseph's Telephone Number	**01483 272449**
St Joseph's Postal Address	**Amlets Lane, Cranleigh, Surrey, GU6 7DH**

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