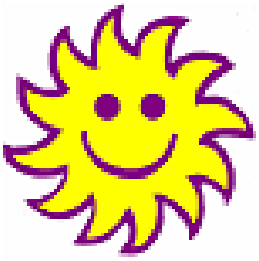

ST JOSEPH'S CATHOLIC PRIMARY SCHOOL

DATA PROTECTION & PRIVACY POLICY & PROCEDURES

Revision History

Version	*Revision Date*	*Revised by*	*Section Revised*
2.0	21st June 2018	Paul Murton	Whole document

Document Control

Document Owner: ***Paul Murton***	***Document No:***	***Status:*** Draft	***Date Approved:***
Security Classification: High/Medium/Low	***Next Review Date:***	***Version:*** V2.04	***Department:***

Contents

1 Policy Statement

The Governing Body 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 Governing Body recognises 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 processed.

The School 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.

2 Purpose

The purpose of this policy is to provide information about our school'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 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.

3 Definitions & Principles

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

- **Personal data:** this refers to any information relating to an identifiable person who can be directly or indirectly identified. It may be held in either paper or electronic records.
- **Processing data:** this refers to anything we might do with personal data, such as holding it, using it, storing it or destroying it.
- **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.
- **Criminal offence data:** this includes data about criminal allegations, proceedings or convictions.

There are certain key **data protection principles** to which the school 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.

4 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.

5 Rights of Individuals

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

5.1 Right of access

You have the right to obtain confirmation from us that your data is processed and to gain access to your personal data by making a subject access request. You should do this by emailing your request to the Data Protection Manager at dpm@stjosephsguildford.com, or by completing a subject access request

form (available on the school website) and sending this to the Data Protection Manager by email to the above address, or by post to the school's address.

We are required to verify your identity before responding, this may mean that we ask you to provide identification documents. Parents may request information relating to their child.

In most cases, we will respond to you within 30 days 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.

Subject Access Requests are always completed within 30-days and are generally provided free of charge. Under legislation, the school can levy a charge for administrative costs if the request is seen as disproportionate and/or is a repeat request from the same person.

5.2 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.
- **Right to withdraw consent:** Individuals have the right to withdraw their consent, where given, at any time.

If you want to exercise any of these rights, you should do so by emailing your request to the Data Protection Manager at dpm@stjosephsguildford.com or by post to the school's address.

6 INTERNATIONAL DATA TRANSFERS

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

7 Our Approach to Data Security and Breaches

Our school 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, disclose or destroy 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 the [school/college/Trust] (for example, for computer maintenance purposes) is strictly regulated and access to data limited;
- staff receive training 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, lockable storage, 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 have been 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;

In the event of a data breach taking place, we will report the circumstances to the Information Commissioner within 72 hours of becoming aware that it has occurred. We will also keep a register of data breaches that have 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.

8 Our Expectations of Staff

We expect all staff working for, or on behalf of, the school, 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 keep work-related personal data on personal devices, such as mobile phones and tablets, or on local computer hard drives or unencrypted USB sticks;
- Take responsibility for ensuring that personal passwords are strong, are changed regularly and never shared;
- 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 Manager.

These rules are an integral part of the school 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.

9 Status of Policy and Review

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

10 DATA PROTECTION OFFICER

St Joseph's Catholic Primary School have appointed a DPO due to the nature of our business activities and/or the services that we provide. We have utilised our existing due diligence measures and procedures, along with extensive employee screening methods, to ensure that the appointed Data Protection Officer has been designated based on their professional qualities.

Data Protection Manager

NAME: _Paul Murton_____

POSITION: _School Business Manager_____

ADDRESS: _St Joseph's Catholic Primary School_____

_155 Aldershot Road_____

_Guildford, Surrey_____

_GU2 8YH_____

EMAIL: _dpm@stjosephsguildford.com_____

TEL: _01483 888401_____

Designated Data Protection Officer

NAME: __Kristy Gouldsmith, Sapphire Consulting_____

POSITION: __Data Protection Officer_____

EMAIL: __dpo@stjosephsguildford.com_____

TEL: __07545 501200_____

11 GOVERNANCE PROCEDURES

11.1 ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of processing undertaken by St Joseph's Catholic Primary School, when required, we carry out risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the GDPR and any codes of conduct that we have obligations under.

We operate a transparent workplace and work diligently to guarantee and promote a comprehensive and proportionate governance program.

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the GDPR and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all staff
- Identify key senior stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that St Joseph's Catholic Primary School has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies (*e.g. Training Policy, Audit Procedures etc*). These measures include: -

- Data Protection (GDPR) & Privacy Policy & Procedure
- Data Retention Policy
- Data Breach Policy
- HR Policy
- Staff Training & Development Policy
- Data Protection Audits & Monitoring Policy & Procedures
- eSafety & Data Security Policy
- Clear Desk Policy
- Appointed Data Protection Officer
- Daily Data Backups

11.2 PRIVACY BY DESIGN

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have additional measures in place to adhere to this ethos, including: -

Data Minimisation

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the GDPR.

Pseudonymisation

We utilise pseudonymisation where possible to record and store personal data in a way that ensures data can no longer be attributed to a specific data subject without the use of separate additional information (*personal identifiers*). Encryption and partitioning is also used to protect the personal identifiers, which are always kept separate from the pseudonymised data sets.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a secondary risk prevention measure for securing the personal data that we hold. Encryption is used to secure off-site digital data storage.

Typically, we utilise encrypted delivery services to transfer sensitive data external Data Processors. These services include, but are not limited to Collect, Perspective Lite, Egress, ESwitch.

Restriction

Restricting access is built into the foundation of St Joseph's Catholic Primary School's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

Hard Copy Data

Due to the nature of our work it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of pupil records, passports, birth certificates).*

This may be required in cases such as Proof of identity, Qualifications, pupil attainment or Religion. Where this is necessary, we transfer the necessary information to digital systems and return original copies.

We operate a strict retention policy and retain data, (whether digital or paper) for the least amount of time consistent with meeting the requirements of the organisation. Paper copies are only retained where legislation requires it.

11.3 Information Flow Audit

To enable St Joseph's Catholic Primary School to fully prepare for and comply with the GDPR, we have carried out a company-wide data protection information flow assessment to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our company in our capacity as a controller/processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from

- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

11.4 Third-Party Processors

St Joseph's Catholic Primary School utilise external processors for certain processing activities. We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes*** *(but is not limited to)**: -***

- IT Systems and Services
- Payroll Services
- Pensions Services
- Human Resources

11.5 Data Retention & Disposal

St Joseph's Catholic Primary School have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and priorities the protection of the personal data at all times.

Please refer to our ***Data Retention Policy*** for full details on our retention, storage, periods and destruction processes.

11.6 Employee Personal Data

As per the GDPR guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook, including relevant Fair Processing Notices that inform them of their rights under the GDPR and how to exercise these rights.

11.7 Security & Breach Management

Where required, we carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

11.8 PASSWORDS

Passwords are a key part of St Joseph's Catholic Primary School protection strategy and are used throughout the school to secure information and restrict access to systems.

11.9 RESTRICTED ACCESS & CLEAR DESK POLICY

St Joseph's Catholic Primary School may on occasions and at its discretion, place all or part of its files onto a secure computer network with restricted access to all/some personnel data. When implemented, access to personal information will only be granted to the person/department that has a specific and legitimate purpose for accessing and using such information.

St Joseph's Catholic Primary School operates a zero-tolerance Clear Desk Policy and does not permit personal data to be left unattended on desks or in meeting rooms, or in visible formats, such as unlocked computer screens or on fax machines, printers etc. Access to areas where personal information is stored (both electronic and physical) are on a restricted access basis with secure controlled access functions throughout the building. Only staff authorised to access data or secure areas can do so. All personal and confidential information in hard copy is stored safely and securely.

12 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by St Joseph's Catholic Primary School to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the GDPR and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes that are detailed in our ***Data Protection Audits & Monitoring Policy***, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Manager has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Governors where applicable. Data minimisation methods are periodically reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting

data subjects and safeguarding their personal data

- To monitor compliance with the GDPR and demonstrate best practice

13 TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the GDPR requirements and its Principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our ***Staff Training & Development Policy*** details how new and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the GDPR requirements and out own objectives and obligations around data protection.

14 RESPONSIBILITIES

St Joseph's Catholic Primary School have appointed a Data Protection Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection. The DPO will work in conjunction with the Data Protection Manager, IT Manager and Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support, mentoring to ensure that they are competent, and knowledge for the role they undertake.