

Data Protection Policy

Context and overview

St John's CE Primary School needs to gather and use certain personal information about individuals. This can include learners, parents, staff and Governors.

All data must be collected, stored and managed in accordance with UK and EU law, and in line with our school ethos and values. Individuals retain the rights over their own data at all times. Our use of their data must be fair and lawful, and we must be open and honest about what we do with people's data.

All data we process is in accordance with the rules as laid down in statute, including the General Data Protection Regulations, the Education Act 1986, the Education and Skills Act 2008 and the Apprenticeship, Skills, Children and Learning Act 2009.

Key principles

- Individuals retain rights over their data
- Data should be collected fairly and lawfully and used only in ways that the individual would expect
- Data should only be kept for as long as is necessary
- Data integrity and security is paramount
- Data governance will be actively managed at all levels of the organisation, to minimise risks to both the individual and the organisation
- All collection and use of data will be open and honest

Why this policy exists

This policy will help ensure that St John's CE Primary School respects the rights of all individuals whose data it collects, including learners, parents, staff and Governors. It encompasses legal responsibilities and best practice. By being open and honest with individuals we will demonstrate that people can trust our organisation and that we handle personal data with integrity. Routine application of these principles will also help protect St John's CE Primary School from the risk of data breaches and unauthorised access to personal information.

Data Protection Law and Principles

The use of personal data is governed by EU and UK law. This is enhanced and explained by case law and best practice.

In order to comply with the law, personal data must be collected fairly and lawfully. It must be stored safely and managed securely. It must not be disclosed to anyone who does not have authority to see it.

The General Data Protection Regulations (GDPR) set out how data should be obtained, stored and handled. These regulations set out six principles that underpin lawful use of data. These provide the foundation for good data governance. These principles are enhanced by a range of powers for individuals to control how data their processed and stored.

Policy Scope

This policy applies to:

- All sites within our organisation
- Our teaching staff, support staff, Trustees and Governors
- Contractors, suppliers and anyone working on our behalf

Responsibilities under this policy

Everyone who works with or for St John's CE Primary School has some responsibility for ensuring that data is handled safely, securely and appropriately.

There are key roles within the organisation that carry specific responsibilities.

The Board of Governors are the strategic lead body for the school. They will bear ultimate responsibility for ensuring that all our legal obligations are met. They will be accountable for any failure to abide by the correct regulations and for any impact that they may have on our learning community and our reputation within the local area.

The Head Teacher and Senior Leadership Team are the operational lead body for the school. They must ensure that all relevant policies and procedures are in place, and that practice follows the policy across all teams and school areas. They will liaise with the Data Protection Officer in the event of any data governance issues that require attention, and will have overall responsibility for setting an appropriate tone of respect for personal data within the school.

The Data Protection Officer, or Data Protection Lead, has a key role to play in providing expert advice and guidance to the Board and the Senior Leadership Team. It is their responsibility to update senior management and the Board about Data Protection issues, and update policies and procedures in accordance with an agreed schedule and following legislative and best practice updates. They will oversee training and guidance for all staff, and be responsible for liaison with 3rd party suppliers, contractors and partners if they handle personal data. They will also oversee and Subject Access Requests, and handle the response to any data breaches, including being the point of contact for the public and notifying the ICO where necessary.

The IT Manager is responsible for ensuring the physical and virtual integrity of IT data storage services, systems and equipment. They will ensure all IT security meets acceptable professional standards, appropriate to the needs of the organisation, and that access to all electronic systems, databases or files is managed in accordance with the relevant policies. They will liaise with any 3rd party used for processing data, such as an HR / payroll supplier or cloud computing provider, to ensure appropriate levels of protection for all personal data. They have responsibility for making sure that customer-facing applications such as websites or online forms comply with relevant regulations including cookie policies and privacy notices. They will also oversee the life-cycle of data, software and hardware, ensuring that the processes for deleting or encrypting files in accordance with Retention Policies function effectively.

What is personal data?

Personal data is information about a person - anything that would allow someone to identify a living individual. Processing that data means obtaining, using, and transferring data, and storing it in any system that allows it to be found again, such as a computer database or filing system.

Our Privacy Notice

St John's CE Primary School will take all reasonable steps to ensure that individuals are aware their data is being processed. This will include telling individuals what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

Our Privacy Notice sets out how we collect data, what data we collect, the lawful basis for that, and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. The Notice will be included in any marketing or information literature the company produces. It will also be available on request, and on the organisation's website.

Keeping personal data secure

Once personal data has been lawfully and fairly collected and processed, it must be safely stored, kept up to date, and safely accessed. Storing data in a way that complies with the regulations is a mix of common sense, clear processes and application of strong IT solutions.

The only people who will have access to personal data at St John's CE Primary School are those who need it for their work. Our IT systems and file storage will have granular levels of permission, and we will ensure that people only see personal data if required for operational reasons and for the benefit of teaching and learning.

Strong passwords must be used to access electronic resources and IT systems. These should never be shared with other people, or written down. St John's CE Primary School will set an appropriate password policy and require passwords to be changed on an annual basis.

Personal data must only be disclosed to those who are authorised to see it, both within and outside the organisation. If there is any doubt about the identity the person requesting access to information, or doubt as to whether they should be allowed to see it, do not disclose information.

Data will only be shared with those people who are authorised to see it. This will be in line with our legal obligations and with the lawful and legitimate requirements of the business. Our Privacy Notice explains who we might share data with, the lawful basis for that, and the circumstances in which you can object to data being shared.

Full training for all staff will be available. This will help them understand their responsibilities under data protection legislation. Staff should ask their line manager or the Data Protection Officer for guidance if they are unsure about any aspect of data protection.

Data use and transfer

Data must only be used for the purpose it was first obtained. Personal data should not be shared informally, either internally or externally to the organisation.

Staff should follow simple checks when transferring data outside the organisation via post or email, to ensure that personal data goes to the correct recipient. St John's CE Primary School will use a simple checklist when sending personal data by post, to add an extra layer of security and checking to our data transfers.

Extra care must be taken when sharing data via email. This might include encryption or use of a secure email client.

Data should not be stored on personal IT devices. In particular staff must not email school documents to their personal email addresses. If data needs to be transferred outside of the secure school environment, staff should use their school email account or a secure cloud storage solution provided by the ICT department.

Marketing and Promotion

St John's CE Primary School does carry out marketing and promotion.

When requesting school visits or brochures, or signing up for more information at Open Days, we will let all prospective parents know how their data will be stored, how often we might contact them, and give them the opportunity to decline to be contacted in the future.

We will ensure that anyone receiving marketing or promotion communications from us has given positive consent to receiving those communications, in the format that we send them out.

All our marketing and promotion communications will include a simple process for being removed from future communications.

CCTV at St John's CE Primary School

St John's CE Primary School does use CCTV cameras on our site. This is to ensure the safety and security of those in our learning community, and to protect the site from damage. Our use of CCTV follows best practice guidelines as laid down by the ICO.

Images recorded by the CCTV cameras are stored on a separate server, in a secure location. They are retained for a maximum of **28** days, after which time they are securely overwritten.

Access to the images is restricted to specified people within St John's CE Primary School. We will only view CCTV footage in response to an incident or an allegation.

The images on our CCTV system are of a sufficient quality to allow us to make out faces of individuals in most circumstances. We are able to take copies of relevant parts of the CCTV footage and store it securely, in order to assist investigations into incidents or allegations.

In certain circumstances we may share CCTV footage with partners or other agencies. This may include senior leaders, parents, the Local Authority or the Police.

You can ask to see CCTV footage in which your image is captured. This should be done in writing as part of a Subject Access Request.

Getting your consent to process your personal data

There may be times where we would like to process your data in a way that requires your consent. This could include taking photographs or images of you engaging in school activities, or adding your contact details to any marketing or promotional mailing lists.

St John's CE Primary School will ensure that we obtain your consent in a positive and clear way. You will be able to refuse consent, and that will not impact your ability to join in the full range of activities and opportunities within the school. We will also ensure that you can withdraw consent quickly and easily, should you change your mind about us processing your data in these ways.

Subject Access Requests

You have the right to ask to see a copy of any information we hold about you. This is known as a Subject Access Request (SAR).

To do this, you can write to us, email us at office@stjohns.worcs.sch.uk, or ring us and talk to one of our office team.