



SCOTT PRIMARY SCHOOL GDPR POLICY – MAY 2018

1 INTRODUCTION

Scott Primary School is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations. We hold personal data about our students, employees, clients, suppliers, in order to fulfil our contractual obligations and to function as a school. This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work.

2 DEFINITIONS

Personal Data - ‘Personal Data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Special categories of personal data - Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data Controller - ‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data Processor - ‘Processor’ means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

Processing - ‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 SUPERVISORY AUTHORITY

This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioners Office].

4 THE PRINCIPLES

Scott Primary School shall comply with the principles of data protection (“the Principles”) enumerated in the EU General Data Protection Regulation (“GDPR”). We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. **Lawful, fair and transparent** - Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. **Limited for its purpose** - Data can only be collected for a specific purpose.
3. **Data minimisation** - Any data collected must be necessary and not excessive for its purpose.
4. **Accurate** - The data we hold must be accurate and kept up to date.
5. **Retention** - We cannot store data longer than necessary.
6. **Integrity and confidentiality** - The data we hold must be kept safe and secure

5 DATA POLICY

5.1 LAWFUL BASIS FOR SHARING DATA

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

Other schools - If a pupil transfers from Scott Primary to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination authorities - This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social workers and support agencies - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division - Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Right to be Forgotten - Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

5.2 Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

6 SPECIAL CATEGORIES OF PERSONAL DATA

What are special categories of personal data?

Previously known as sensitive personal data, this refers to data about an individual which is more sensitive, so requires more protection. This includes data such as that relating to race, ethnic origin, or any other sensitive information about an individual.

7 RETENTION OF RECORDS

Records detailing contracts and are kept in line with standard retention periods in order to comply with legal and financial compliance.

8 PROTECTION OF RECORDS

Staff are issued with laptops which are locked down in line with internal policies, with patch management, Anti-Virus, and configuration management agents. Data stored on devices is minimised, with VPN configuration allowing access back to school shared areas. Log files record access to endpoints with the software installed.

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be saved to their school provided account via Google Drive
- If information is being viewed on a mobile device, staff will have to agree to Google adding security measures to their devices.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

9 HOW WE DEAL WITH SUBJECT ACCESS REQUESTS

Scott Primary School will provide an individual with a copy of their personal information if requested. This will be supplied within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats. If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

10 STAFF TRAINING AND AWARENESS

Scott Primary School staff are trained in the core principles of data management and GDPR.

Staff access to sensitive data will occur in the nature of providing information when requested by school staff, configuring access to and testing access to data. Staff will not disclose, share or duplicate data, and will report to the Schools DPO or responsible person on any issues they identify where data is being misused by school staff.

11 SAFEGUARDING

Scott Primary School has a defined Safeguarding Policy available from the website or on request. All staff receive training on Safeguarding and Child protection.

12 EQUIPMENT REMOVED FROM SITE

Removing equipment for repair is avoided if possible, with repairs conducted on the customer site. On occasions where it is agreed to be necessary to remove school equipment, it will be stored in secure workshop facility. Where the equipment contains data, and is deemed beyond economical to repair, this will be returned to site to be processed by the customers approved WEEE registered carrier.

13 3RD PARTY SUPPLIERS AND TOOLS

Scott Primary School undertake a rigorous process of reviewing 3rd Party Suppliers and sub-contractors prior to undertaking any activity with them.

Suppliers are reviewed as part of the Supplier review processes in maintaining the ISO 9001:2015 accreditation.

Supplier review processes include enhanced analysis of a supplier's data policy and commitment to GDPR. Any supplier that does not satisfactorily demonstrate a commitment to data and privacy protection will not be considered as a partner of Scott Primary School.

14 CONTACT

If you wish to contact us to make a Subject Access Request, request rectification or object, please contact our office on office@scottprimary.co.uk