POTT SHRIGLEY CHURCH SCHOOL

'Be kind and compassionate to one another, forgiving each other, just as in Christ, God forgave you"

GDPR Policy (Spring 2024)

This policy sets out how the school deals with personal information correctly and securely and in accordance with the General Data Protection Regulation, and other related legislation.

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The data controller
5. Data protection principles
6. Roles and responsibilities
7. School Specific Data Security Measures
8. Data breaches
9. Training
10. Complaints
11. Contacts

1. Aims

Our School will comply with the demands of the General Data Protection Regulation (GDPR) to be known as the Data Protection Act 2018. Members of staff will gain familiarisation with the requirements of the GDPR either in a staff briefing or as part of their induction.
This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy follows guidance issued by the Information Commissioner's Office (ICO) and the Department for Education (DfE).
The school is a Data Controller as data is processed - that is the personal information of pupils, families, staff, visitors and other school users.
The school is a Data Processor as it processes data on behalf of other public bodies such as the DfE.

3. Definitions

Term	Definition
Personal data	Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.
Sensitive personal data	The GDPR/ICO requires that particular care is taken with the following data: • Data regarding children • Health (physical, mental, genetic) • Ethnicity • Religion • Sexuality • Performance management and trade union membership
Consent	Must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available to an audit. A person must be 13 years old in order to record their consent.
Processing	The acquisition, storage, processing and transmission of data
Cross-border processing	The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area)
Data subject	Any identifiable person whose data is processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Filing system	Any structured set of personal data, however stored in any format (physical or digital) that can be processed.
Personal data breach	A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data. Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

Pseudonymisation	The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.
Legal basis	The school decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties, the school uses the following bases for processing and controlling data : • Legal basis: Public Task • Admissions • Attendance • Assessment • Pupil and staff welfare • Safe recruitment • Staff training • Performance Management • Legal basis: Consent • Various uses of photographs and moving images • Trade union membership • Staff ethnicity, religion and health data (Note the Staff Privacy Statement) • The use of data to promote the social life of the school community Legal basis: Contract • When processing is required to carry out the performance of a contract
Password protection	The act of 'locking' a device or document. The information remains readable beyond the password.
Encryption	The act of encoding all the information beyond a password or code.
Data portability, data subject access request	Data subjects (or a child's parents) may request access to a copy of all their data. The school has established an efficient means of accomplishing this task which may not carry a charge and will be completed within 15 working days. Data subjects may request that data is brought up-to-date or made more accurate. *(FN 1)*

4. The data controller

Our school collects, processes and uses personal information relating to pupils, staff, governors and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Data Protection Officer, currently the Headteacher. The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

5. Data protection principles

• Personal data must be processed lawfully, fairly and transparently

• Personal data can only be collected for specific, explicit and legitimate purposes

• Personal data must be adequate, relevant and limited to what is necessary for processing

• Personal data must be accurate and kept up-to-date

• Personal data may identify the data subject only as long as is necessary for processing

• Personal data must be processed in a manner that ensures its security

• Any breaches in data security must be reported to the ICO within 72 hours

• The school must report any breaches caused by third parties who have access to school users' data within 72 hours.

• The school must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information

(FN 2)

Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The school's Privacy Statements set out in detail how the school will maintain the security of school users' data. The Acceptable Use Policies set out the duties of the staff and other school users in supporting data security.

Within school the security of data is coordinated by the Headteacher.
The Governor with special responsibility for data security is Jane Langdon.

The school has appointed a Data Protection Officer who has responsibility for overseeing the implementation of this policy and all GDPR related documents. The DPO will monitor compliance, report to the school leadership and support the school with updates and interpretations as the GDPR develops.

The DPO will liaise between the school and the ICO and must be informed as soon as is practicable of any personal data security breach.

The DPO will support the school in its communication with schools users (pupils, families, parents, governors, contractors and visitors) about the school's GDPR procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects rights.

Data subject requests should be made in writing to the DPO. The DPO might have to respond to any or all of the following

- Why the data is processed
- On which basis
- Who has seen it
- How long it will be stored for
- Where the data was sourced
- Whether decisions have been based on the data

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by parents. The school may take into account the views of a pupil.

The school's DPO is:
Mrs Lisa Paton – School Bursar
Staff should contact the DPO should they believe that this policy and/or the privacy statements and/or the acceptable use policies are not being followed.

Data Audit
The school will carry out a data audit at the beginning of each school year. Within the audit the school will record all third parties' compliance with the GDPR if those third parties process data for any school users. Such confirmation will, from now on, be an essential part of any contract with third parties when the processing of school users' data is involved. The school will not share data, or have any data processed, by any third parties who do not confirm their compliance with GDPR requirements.
Preferably companies that process school users' data will have certification to ISO27001. The audit will also check the security of physical and digital records and devices.

Processing Records
To meet the ICO's recommendation that 'scrupulous records' are developed the school will record its processing of data and the results of its data audit. It will record the ongoing security measures for physical and digital filing systems. Confirmation of compliance by third parties accessing any school user data will be recorded.
In broad terms the school will record which data has been processed (including deletions when data should no longer be stored) on which legal basis.
Consent replies are recorded within the system.

Sharing Data
Personal data may be shared with third parties:

- To protect the vital interests of a child
- To protect the vital interests of a member of staff
- To prevent or support the detection of fraud or other legal proceedings
- When required to do so by HMRC

CCTV
CCTV is used to support the safety and security of school users. We adhere to the ICO's code of practice for its use.

Photographs and moving images
Consent is requested from parents and staff for the use of images. Letters requesting consent outline the choices that pupils and staff may make for the use of their images.
The school may seek consent to use photographs for the following purposes:

- To support school user welfare (identity and security)
- To celebrate achievement within the classroom
- To celebrate achievement within the school
- To celebrate achievement in the printed press
- To celebrate achievement online

7. The school's specific data security measures - data protection by design

A. All IT systems - mobile devices, laptops, mobile phones and any device capable of processing data, will be password protected.

B. All IT systems will be kept securely, and desktop computers and portable devices will be sited/stored in secure places.

C. Staff are expected to ensure the safety of their allocated school devices: devices may not be left unattended in cars at any time and they must be kept out of sight if taken home.

D. All passwords must be 'strong and not contain any related words to the person or organisation;', the school will require regular changing of passwords – at least once every half term.

E. No passwords will be written down or shared; advice is available on the safe storage of passwords.

F. The school will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.

G. All deleted data will be deleted in a secure manner: physical data will be shredded and digital data will fully deleted with trash / junk emptied regularly. Only data that is necessary for the effective performance of the school will be processed.

H. Data protection will be integrated into all appropriate policies and procedures (e.g. staff induction).

I. Staff will be updated with any significant interpretations or developments of the GDPR.

J. The school will have data impact assessments in place to protect vulnerable data subjects and sensitive data.

K. Data contained within an email, or attached to an email, will be transferred to a secure folder and the email deleted.

L. Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support a school user's needs, but not to others.

M. All school users will handle personal data with care: it will not be left unattended (unattended computers must be locked), school users will not allow others to oversee personal data (screens must be positioned with care); papers must not be left where others can see them.

N. All computers that might be used to process data will be set to lock (a screensaver will activate) after 10 minutes of inactivity.

O. The Headteacher and/or the DPO will approve who and how personal data is stored on mobile devices. All school ipads can be wiped remotely.

P. Personally owned devices will not be used for the storage of school personal data.

8. Data breaches

All staff must report to a member of the SLT or the DPO any suspected data breaches (the loss, theft, unauthorised access to data etc.) immediately. It will be for the SLT/DPO to decide whether to the suspected data breach warrants reporting to the ICO. NB a data breach would include the accidental sharing of personal data via a wrongly addressed email.

9. Training

All staff will receive basic training in the requirements of the GDPR. The training will be recorded in the data audit and/or the data processing records. Governors will also receive a briefing. Data protection will form a part of pupils' e-safety education. The school will keep staff and governors up to date with guidance, changes and interpretations to data protection law.

Data Protection Impact Assessment
For the school's most sensitive data processing activities the school will have completed a DPIA to ensure that the risk to individuals of a data breach is minimised, as should be the risk to the school's reputation. Staff involved in processing the school's most sensitive data will have to record their reading and understanding of the relevant DPIA.

Monitoring The DPO will lead the formal monitoring of the school's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.

10.Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

11.Contacts

If you have any enquires in relation to this policy, please contact Mrs Anne-Marie Willis (Head Teacher) or Mrs. Paton (Bursar)

Footnotes

1. Data subjects' rights include • The right to be informed • The right of access • The right to object • The right to be forgotten (this might prove impossible in the school context) • The right of rectification (any inaccurate data must be corrected)	2. In deciding whether to pass on a suspected data breach to the ICO the DPO will consider whether the data breach might affect a person's • Reputation • Confidentiality • Financial wellbeing • A loss of control over their data • Make them vulnerable to discrimination • Their rights and freedoms

Written – Spring 2024
Written by – Anne-Marie Willis and Lisa Paton (Headteacher ICO and Bursar DPO)
Approved by – Jane Langdon (Chair of Governors)

This policy will be renewed every three years or sooner if significant changes are made to General Data Protection Regulation, or other related legislation.