PENWORTHAM PRIMARY SCHOOL

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY & HANDBOOK

DEFINITIONS

- Data Subject – person whose data you hold
- Data Controller – organisation
- Data Processor – organisation who holds and shares information
- Processing – obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, matching, transmitting, disseminating, making available, aligning, combining, blocking, erasing & destroying
- Personal data – any information relating to an identified or identifiable natural person, e.g. name, identification number, location data, online identifier
- Consent: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'
- Personal Data Breach – 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

PURPOSE OF GDPR – THE PROTECTION OF NATURAL PERSONS IN RELATION TO THE PROCESSING OF PERSONAL DATA

PRINCIPLES

1. Lawfulness, Fair & Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality

School will review annually which data is collected. Personal data shall be processed lawfully (Section 29 of DPA). **Consent will be sought unless the data is statutory**. Parents are able to withdraw consent at any time. Privacy Notices will be distributed to parents (on behalf of the child) and staff.

RETENTION OF DATA

- Data will be retained within an organisation. Dependant on what the information is there are different periods of time for certain data.
- Information Society Services are defined as any service normally provided for remuneration, at a distance, by electronic means. This includes all social media usage, any software/programmes used and iCloud storage. School will ensure that they are compliant with GDPR, a contract will be made and time frames identified re: how long records will be kept. Email accounts need to be compliant; therefore School will use the lancs.sch.uk, Office 365 accounts.
- Schools will ensure that we work in a transparent way; ensuring parents understand what we do with the data, why we need/collect the data and how it will be used.
- School will follow guidance from the ICO (Information Commissioner's Office).
- School will complete a data map. This records: why, whose, what, when, where.
- It is essential that school will not extract information/data unnecessarily, therefore minimising excessive collection. This is strategic information management.

PROHIBITION

Special categories are:

- Racial/ethical origin, Political opinions, Religious/philosophical beliefs, Trade Union membership, Genetic/Biometric data, Health data (unless the School has a separate agreement with the School Health team re: information sharing) and Sex life/sexual orientation.
- GDPR requires that School 'Processes data in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.'
- Electronic records must be password protected. At School we will store information on our shared server via Microsoft Office 365 services. All laptops/electronic devices will be password protected (this may include the occasional use of password protected pen-drives) with anti- virus software installed. No data will be stored on personal electronic equipment. Therefore, as a School we are able to ensure that we maintain confidentiality, integrity, availability and resilience. School will request that the IT Technical provider carry out regular testing, assessing and evaluation of measures.

SHARING INFORMATION

Staff will receive regular training and information regarding changes/updates to the GDPR. If staff have questions they must seek advice from the DPO and reference the document ICO – Data Sharing Code of Practice. **(Appendix 1A & 1B for checklist).**

- Third party data processors will be required to meet all GDPR requirements.
- Data sharing out of the EU requires the School to notify all Data Subjects.

School has the following policies and processes to uphold GDPR:

1. Privacy Notices
2. Data Protection Policy and Procedures
3. Retention Schedules
4. Processes to accommodate data subject rights
5. Incident reporting
6. Data Protection Impact Assessments
7. Staff Training

ACCESS/RIGHTS

Controllers have a legal obligation to give effect to the rights of Data Subjects;

- Fair processing notices are re-cast as a right
- Rights of subject access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restrict/object
- Right to data portability
- Right not to be profiled (automated processing of personal data)

All Data Subjects have the right to access of their records. The information can be accessed with no fee however copies made are chargeable (price: £10). This process usually is given a 1 month

time scale, however in certain complex circumstances this may be a period of 2 months. All Subjects have a right to a fair processing of information.

Exemptions:

- Crime
- Disclosure by law
- Judicial proceedings
- Crown honours & dignities
- Armed Forces (defence purpose)
- Economic well-being
- Legal Professional Privilege (LPP)
- Negotiations
- Research & Stats

OBLIGATION

School has an obligation to appoint a Data Protection Officer (DPO). The DPO will carry our regular and systematic monitoring of data subjects on a large scale, looking into special categories and personal data relating to criminal convictions & offences.

School will appoint a DPO by means of a 'Buddy' system within WRIST. Each school will team with another school to provide support and guidance. **(Appendix 2 for contact details).**

The role of the DPO is:

- the first point of contact for the School and ICO
- has knowledge and understanding of the DPA
- understands the School's structure
- is familiar with School's IT infrastructure and technology
- is independent of decision making
- has the ability to advise the School (with the support from the LA legal team)
- provide advice for the Data Protection Impact Assessments (DPIA) – these are to be completed when necessary

Procedure for Breach Reports:

- Report to ICO within 72 hours (not investigate)
- Information to gather for ICO – nature of incident, categories and numbers of records, ID of School, likely consequences for Data Subjects & measures taken
- High risk data – inform Data Subjects without undue delay

Powers of ICO:

- Information Notice
- Assessment Notice
- Enforcement Notice
- Penalty Notice
- Powers of entry & inspection (warrant)

References:

Information Commissioner's Office - https://ico.org.uk/
Information and Records Management Society - http://irms.org.uk/
GDPR in Schools - https://www.gdpr.school/

Appendix 1A

Data Sharing Checklist – Systematic Data Sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis.

Is the sharing justified? Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share? Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share.

It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Appendix 1B

Data Sharing Checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances.

Is the sharing justified? Key points to consider:

Do you think you should share the information?
Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
Do you have concerns that an individual is at risk of serious harm?
Do you need to consider an exemption in the DPA to share?

Do you have the power to share? Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share. Key points to consider:

- What information do you need to share? – Only share what is necessary. – Distinguish fact from opinion.
- How should the information be shared? – Information must be shared securely. – Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision.

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Taken from ICO Data Sharing Checklists
https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf

Appendix 2

DPO Information:	
Name	Miss K Penarski
Telephone Number (work/mobile)	01772 743321
Email address	head@penwortham-pri.lancs.sch.uk
Date of appointment as DPO and review date	February 2026. Review September 2027
Address	c/o Penwortham Primary School, Crookings Lane, Penwortham, PR1 0HU.
Job title	Headteacher