



DATA PROTECTION (DP) FRAMEWORK- ADOPTED FROM EDUCATION DATA HUB- (version 6)

Item	Detail
Last Reviewed	07/2026
Reviewed By (Name)	Leah Slack School Business Manager
Approved by/ date:	Governors Sept 2026
Next Review Date	07/2027

Contents of this Framework (related documents)

Data Protection Policy

Annex 1: Legal Conditions for Processing

Annex 2: Personal Data Breach Procedure (including Cyber Incidents)

Annex 3: Data Protection Impact Assessment Procedure

Annex 4: Data Protection Impact Assessment Guidance

Annex 5: Requests under the Freedom of Information (FOI) Act 2000 / Environmental Information Regulations (EIR) 2004

Annex 6: Data Protection Complaints Policy

FOI Publication Scheme

Privacy Notice (Pupil & Family)

Privacy Notice (Workforce)

Privacy Notice (Governors/Trustees/LGB members)

Privacy Notice Pupil Friendly

Addendum to Child Protection policy regarding Records Management

Records Retention Schedule

Social Media Policy

CCTV Policy

Special Category Data Policy

Remote Learning Policy

Artificial Intelligence Policy

AI Strategy

Pupil Guide to AI Use

Photo Policy

IT Disaster Recovery Procedure and Plan

Introducing our DP Framework

This framework comprises of a number of key documents; including our Data Protection policy and other associated policies and procedures, which together form the school's commitment to protecting the data of its pupils, families, staff and volunteers.

Compliance with this framework is mandatory for all staff.

"Personal data" means **any** information where a living person is either identified or identifiable, from the information alone, or with other information – these are known as Data Subjects.

Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in Social Media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system, or intended to be filed).

"Special category data" is personal data that needs more protection because it is sensitive.

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data.

"Data Subjects" include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

"Data Controller" means the school, alone or jointly with other Data Controllers, decides on why and how personal data is processed.

"Processing" means collecting, storing, using, sharing and disposing of data.

"Processors" are the external bodies who processes personal data on behalf of the controller.

"Staff" includes current or former; permanent employees, temporary staff, agency staff, consultants, governors, volunteers, and anyone else working for the school. We will also expect job applicants and contractors (and their staff) to comply with this policy.

"Data Protection Officer" (DPO) is a statutory role with responsibility for:

- advising the school about data protection obligations,
- dealing with breaches, including suspected breaches and identified risks
- monitoring compliance with this policy.

Our Data Protection Officer is: [*Education Data Hub | Derbyshire County Council | County Hall, Matlock, Derbyshire DE4 3AG | 01629 532888 dpforschools@derbyshire.gov.uk*]

"Data Protection Lead" is Leah Slack and is the member of school staff nominated to manage communication with the DPO.

Responsibilities

All staff are responsible for reading and understanding this framework before carrying out tasks that involve handling personal data, and for following this framework, including reporting any suspected breaches to our Data Protection Officer.

All leaders are responsible for ensuring their team sign to confirm they have read, understood and will comply with the documents in this framework, before carrying out tasks that involve handling personal data, including reporting any suspected breaches.

DP Legislation & Regulator

1. Relevant legislation includes, but is not limited to:

- Section 3 of the European Union (Withdrawal) Act 2018 (incorporates General Data Protection Regulation (EU) 2016/679 into the law of England and Wales, Scotland and Northern Ireland, to be known as the UK GDPR)
- General Data Protection Regulation (GDPR);
- Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;
- Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing (“marketing” includes fundraising and promoting an organisation’s aims, not just selling.)
- Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
- Human Rights Act 1998
- Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials.
- Protection of Freedoms Act 2012
- Data (Use and Access) Act 2025

2. In the UK, the Information Commissioner’s Office (ICO) is the data protection regulator.

3. Breaches of data protection legislation can cause the risk of real harm to people whose data is handled in an unfair or unlawful way, as well as significant monetary penalties and damage to reputation.

4. Individual members of staff may be prosecuted for committing offences under Sections 170, 171 or 173 of the DPA 2018. These offences are: obtaining, disclosing, altering or retaining data without the consent of the Data Controller; purposefully identifying people from data that has been “de-identified”; and purposefully withholding data that a data subject has requested, and is entitled to receive.

Policy Statement

At **The Park Schools Federation**, we recognise that the effective management of personal information is fundamental to safeguarding pupils, supporting their education, maintaining public trust and fulfilling our statutory responsibilities. The Federation is committed to ensuring that personal data is processed lawfully, fairly, transparently and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant education legislation. The Federation promotes a culture of accountability, confidentiality and information security, ensuring that all members of the school community understand their responsibilities when handling personal information. Data protection considerations are embedded within decision-making, safeguarding arrangements, curriculum delivery, school administration and the wider governance of the Federation.

Leadership and Governance

The Governing Body, Headteacher and Data Protection Officer work together to ensure effective information governance across the school. Leaders regularly monitor compliance, review procedures and evaluate risks to ensure that personal information is protected and used appropriately. Data protection forms part of the school's wider safeguarding and risk management framework, and leaders ensure that information management arrangements remain effective, proportionate and responsive to emerging risks. Staff are provided with clear guidance, support and training to enable them to fulfil their responsibilities confidently and consistently.

Safeguarding and Child Protection

The school recognises that information sharing is often essential in promoting the welfare and safeguarding of children. Personal information will be shared with relevant agencies where there is a lawful basis to do so and where sharing is necessary to protect a child or fulfil statutory duties. Staff receive training to ensure they understand the relationship between data protection legislation and safeguarding responsibilities, recognising that data protection law does not prevent the appropriate sharing of information where a child may be at risk of harm. Accurate and timely record keeping supports effective safeguarding practice and helps ensure that children receive appropriate support and protection.

Staff Training and Awareness

All staff, governors and relevant volunteers will receive data protection training appropriate to their role and responsibilities. Training will be provided during induction and refreshed annually. Additional training will be delivered where legislative updates, technological developments or identified risks require enhanced understanding. Through ongoing professional development, the school seeks to ensure that all staff understand how to handle personal information securely, recognise potential breaches and respond appropriately to information governance concerns. Training records will be maintained and monitored as part of the school's compliance arrangements.

All Staff Will

All staff at The Park Schools Federation are responsible for ensuring that personal information is handled lawfully, fairly, securely and in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, Article 8 of the Human Rights Act 1998 and Federation procedures. Staff will understand that data protection is a shared

responsibility and forms an important part of safeguarding, information security and professional conduct.

All staff will:

- Comply with the requirements of data protection legislation and respect the privacy rights of all individuals whose personal data is processed.
- Ensure that pupils, parents, carers, staff and other data subjects have access to relevant and up-to-date privacy notices explaining how their information is used.
- Consider data protection implications when introducing new processes, systems or ways of working involving personal data and participate in risk assessments where required.
- Collect, use and retain only the minimum amount of personal information necessary to fulfil their professional responsibilities.
- Record information, opinions and professional observations accurately, objectively and respectfully, recognising that records may be disclosed to the individual concerned.
- Take reasonable steps to ensure that personal information is accurate, current and corrected promptly when inaccuracies are identified.
- Process personal data using an appropriate lawful basis and seek consent only where consent is the appropriate legal basis for processing.
- Obtain appropriate consent before personal information is used for promotional, publicity or marketing purposes.
- Ensure that consents are reviewed and renewed in accordance with Federation procedures and legal requirements.
- Review personal information regularly and ensure records are retained and securely disposed of in accordance with the Federation's retention schedule.
- Immediately refer requests for access to personal data to the appropriate member of staff so that Subject Access Requests can be handled in accordance with legal requirements.
- Carefully consider data protection obligations before disclosing information relating to another individual and seek advice where necessary.
- Respect and appropriately respond to requests from individuals exercising their rights under data protection legislation.
- Access only the personal information required to fulfil their role and never attempt to view records without a legitimate educational or business need.
- Follow all Federation security procedures, access controls and system guidance designed to protect personal information.
- Share personal data with external agencies or organisations only where an appropriate information-sharing agreement exists or where authorisation has been provided by the Data Protection Officer or Senior Information Risk Owner (SIRO).

- Ensure that the recording, monitoring and use of emails, telephone calls, internet activity, CCTV footage and other electronic records complies with legal requirements and Federation procedures.
- Complete mandatory data protection and information security training and participate in refresher training as required.
- Use data matching or data analysis techniques only for authorised purposes and in accordance with relevant procedures and legal requirements.
- Support the Federation in maintaining accurate information governance records and regulatory registrations where required.
- Follow approved procedures when anonymising or pseudonymising personal information for research, reporting or statistical purposes.
- Seek advice from the Data Protection Officer before transferring or sharing personal data outside the United Kingdom.
- Recognise Special Category Data, including information relating to health, ethnicity, religion, biometrics and other sensitive information, and ensure that such data is stored, accessed and shared only by authorised persons with a legitimate need to know.
- Ensure that Special Category Data is clearly marked as confidential or "OFFICIAL-SENSITIVE" where appropriate and transferred using secure methods.
- Report any actual, suspected or potential data breach immediately in accordance with the Federation's Data Breach Procedure.

Failure to comply with this policy may result in disciplinary action and, in serious cases, referral to external regulatory or law enforcement agencies. All staff are expected to maintain the highest standards of confidentiality, professionalism and information security at all times.

Data Protection by Design and Risk Management

The school will embed data protection considerations into the planning and implementation of new systems, technologies, projects and initiatives. Data Protection Impact Assessments will be undertaken where processing activities are likely to present a risk to individuals' rights and freedoms. Leaders will ensure that risks are identified, assessed and mitigated effectively, and that only the minimum amount of personal information necessary for a specified purpose is collected and retained. Regular reviews of data handling practices help ensure that information remains accurate, relevant and secure.

Data Breach Management and Reporting

The Park Schools Federation recognises that a personal data breach can have significant consequences for pupils, parents, staff and the Federation. A personal data breach is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information held by the Federation. This may include information being sent to the wrong recipient, the loss or theft of devices containing personal data, unauthorised access to records, cyber security incidents, or the inappropriate sharing of confidential information. [\[data-protection-policy | PDF\]](#)

All staff, governors, volunteers and contractors have a responsibility to report actual, suspected or potential data breaches immediately upon discovery. Staff must not attempt to conceal errors or resolve serious incidents independently. Any concern must be reported to the Executive Headteacher and Data Protection Officer (DPO) without delay to enable prompt investigation and action. [\[data-protection-policy | PDF\]](#)

Upon notification of a breach, the Federation will take immediate steps to contain the incident and minimise any potential harm. This may include recovering information, recalling emails, changing passwords, suspending access to systems, securing equipment, or contacting affected individuals where appropriate. The Federation will investigate the cause, nature and extent of the breach and assess the potential impact on the rights and freedoms of those affected. [\[data-protection-policy | PDF\]](#)

The Data Protection Officer, in consultation with the Executive Headteacher, will determine whether the breach meets the threshold for reporting to the Information Commissioner's Office (ICO). Where required by law, reportable breaches will be notified to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the incident. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, affected persons will also be informed promptly and provided with appropriate advice and support. [\[data-protection-policy | PDF\]](#)

A record of all data breaches, including near misses, will be maintained by the Federation. This record will detail the nature of the incident, actions taken, outcomes of investigations and any lessons learned. Following a breach, the Federation will review its policies, procedures, training and technical safeguards to reduce the likelihood of recurrence and to strengthen information security arrangements. [\[data-protection-policy | PDF\]](#)

Deliberate, reckless or negligent breaches of this policy may result in disciplinary action and, where appropriate, referral to external agencies. The Federation expects all members of the school community to play an active role in protecting personal information and promoting a culture of confidentiality, accountability and data security. [\[data-protection-policy | PDF\]](#)

Data Breach Response Procedure

In the event of a data breach, staff must:

1. Immediately report the incident to the Executive Headteacher and Data Protection Officer.
2. Take reasonable steps to contain the breach where it is safe and appropriate to do so.
3. Preserve any evidence relating to the incident.
4. Avoid discussing the breach with unauthorised individuals.
5. Cooperate fully with any investigation.
6. Follow all instructions provided by the Executive Headteacher, Data Protection Officer or Federation leadership team.
7. Complete any required incident reporting documentation.

This procedure forms part of the Federation's wider safeguarding, risk management and information governance arrangements and supports the Federation's duty to protect the personal information entrusted to it. [\[data-protection-policy | PDF\]](#)

Supporting Pupils and Families

The school is committed to processing personal information in a way that supports pupils' education, wellbeing and inclusion. Information is used responsibly to enable appropriate teaching, assessment, safeguarding, attendance monitoring, pastoral support, SEND provision and communication with parents and carers. The school seeks to maintain open and transparent relationships with families through clear privacy notices and by ensuring that individuals understand how their information is used and protected.

Monitoring, Evaluation and Continuous Improvement

The effectiveness of the school's data protection arrangements will be reviewed regularly through monitoring activities, policy reviews, staff feedback, training evaluations and the investigation of incidents or near misses. Lessons learned from audits, complaints, breaches or changes in legislation will inform future improvements. School leaders and governors will use this information to ensure that information governance arrangements remain effective, proportionate and reflective of best practice.

Policy Review

This policy will be reviewed annually by the Headteacher, Data Protection Officer and the designated governor with responsibility for data protection. The review process will consider legislative changes, guidance issued by the Department for Education or Information Commissioner's Office, audit findings, breach records and feedback from stakeholders. Any significant amendments will be approved by the Governing Body to ensure continued compliance and effectiveness.