

Data Protection Policy

2026-2028

Contents	Page
1 Introduction	3
2 Scope of this policy.....	3
3 Data protection principles.....	3
4 Responsibilities of staff and contractors.....	3
5 Data Security.....	3
6 Sending personal data securely.....	4
7 Data subject rights	4
8 Prohibited activities.....	5
9 Privacy by Design.....	5
10 International transfers	6
11 Conclusion	6
12 Definitions	7

1 Introduction

Our school is committed to protecting the rights of all individuals in relation to the processing of their personal data. The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with this policy and relevant legislation.

2 Scope of this policy

This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing personal and special category data to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended from time to time

This policy and the legislation apply to all personal data, both that held in paper files and electronically. So long as the processing of the data is carried out for school purposes, it applies regardless of where data is held.

‘Processing’ data is widely defined and includes obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

2.1 Legislation and guidance

This policy is based on the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended from time to time.

It also reflects guidance published by the Information Commissioner’s Office (ICO) and, where relevant, Department for Education (DfE) guidance on the safe and appropriate use of technology and data in education.

Where the school uses specific technologies or processing activities (for example CCTV, biometric recognition systems, photography/video, or emerging technologies such as artificial intelligence), we will also comply with any additional legal requirements and relevant statutory or regulatory guidance that applies to those activities.

3 Data protection principles

Personal and special category data must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

3.1 Collecting personal data (lawful basis)

We will only process personal data where we have a lawful basis to do so under data protection law. The lawful bases include:

- Consent: the individual has freely given clear consent for us to process their personal data for a specific purpose
- Contract: processing is necessary for a contract with the individual, or because they have asked us

to take specific steps before entering into a contract

- Legal obligation: processing is necessary for us to comply with the law
- Vital interests: processing is necessary to protect someone's life
- Public task: processing is necessary for us to perform a task in the public interest or in the exercise of official authority
- Legitimate interests: processing is necessary for our legitimate interests (or those of a third party) and those interests are not overridden by the individual's rights and freedoms

Where we process special category data (for example information about health or ethnicity) we will also ensure an additional condition for processing under data protection law applies. Where we process criminal offence data, we will ensure the relevant legal requirements are met.

When we first collect personal data directly from individuals, we will provide appropriate privacy information explaining how and why we use their data.

Staff must only collect and process personal data where it is necessary for their role and must ensure data is accurate and kept up to date. Where data is no longer required, it must be securely deleted, anonymised or otherwise handled in line with the school's retention arrangements.

4 Responsibilities of staff and contractors.

4.1 Governing board

The governing board has overall responsibility for ensuring that the school complies with its data protection obligations, including ensuring appropriate policies, procedures and training are in place.

4.2 Data Protection Officer (DPO) & Data Protection Lead (DPL)

The school has appointed a Data Protection Officer (DPO) to oversee compliance with data protection legislation and this policy. The DPO provides expert advice, monitors the school's compliance, supports the completion of Data Protection Impact Assessments (DPIAs), and acts as a point of contact for data subjects and the Information Commissioner's Office (ICO).

The school's Data Protection Lead (DPL) is a member of the Senior Leadership Team and is responsible for leading operational data protection activity within the school. The DPL works closely with the DPO, ensuring that data protection requirements are implemented effectively and that any issues are escalated appropriately.

DPO contact details:

Name: Paula Creighton

Email: paula.creighton@sptcompliance.co.uk

DPL contact details:

Name: Zainul Haque

Email: zhaque@icknield.beds.sch.uk

4.3 Head Teacher

The Head Teacher acts as the representative of the data controller on a day-to-day basis and is responsible for ensuring that appropriate arrangements are implemented across the school.

4.4 All staff, contractors and volunteers

All staff, contractors, governors and volunteers are responsible for handling personal data in accordance with this policy and for raising concerns promptly where they believe personal data may have been misused, lost, disclosed in error, or otherwise put at risk.

Staff and contractors must:

- Complete the Data Protection training as soon as they join the school. This is a mandatory requirement.
- Complete an annual refresher course as directed by their manager
- Ensure that they only ever process personal data in accordance with requirements of the relevant legislation.
- Follow the 6 Principles highlighted above and must seek advice where required.

5 Data security

Keeping personal data properly secure is vital to comply with data protection legislation. All staff and contractors are responsible for ensuring that any personal data we have access to is kept securely. We are also responsible for ensuring that personal data is not disclosed inappropriately (either orally or in writing) whether intentionally or accidentally, to any unauthorised recipient or third party.

This includes, as a minimum:

- We should always keep passwords safe and never share them
- Lock away any personal data kept in paper format in a lockable cabinet or pedestal. Do not leave documents on desks unattended at any time
- If it is necessary to take hard copy documents out of the school make sure that those documents are always looked after, this includes notebooks and files. Consider whether it is necessary to take files out of the school at all or if so, take them on an encrypted laptop.

5.1 Storage of records

Personal data will be stored securely, whether in paper or electronic form. Access to personal data will be restricted to those who require it for a legitimate school purpose.

Where personal data is stored electronically, it must be saved to approved school systems and locations. Staff must not store personal data on unauthorised devices, personal cloud storage, or personal email accounts.

5.2 Retention and disposal of records

Personal data will be retained only for as long as necessary for the purpose(s) for which it was collected and in accordance with the school's retention arrangements.

When personal data is no longer required, it must be securely disposed of. Paper records must be shredded or otherwise securely destroyed. Electronic records must be securely deleted or anonymised.

Where disposal is carried out by a third party, the school will ensure appropriate assurances and arrangements are in place to protect the data during disposal.

5.3 Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Any actual or suspected data breach must be reported immediately to the DPO / Data Protection Lead. The school will investigate, take steps to contain the breach, assess risk, and report to the ICO and affected individuals where required by law.

A detailed procedure for managing personal data breaches is set out in Appendix A.

6 Sending personal data securely

We can send documents containing personal data securely using the following methods:

Requested by:	Method:
Hard copy	Documents should be hand delivered to the data subject wherever possible. Make sure that the documents are securely contained in a sealed envelope and signed for. If it not possible for the data subject to collect the documents themselves use the special delivery service. Note: Check you have the correct address before posting
Email	This is the preferred method. Scan a copy of the file and move it to a secure location on the school's network. Send the file by secure data transfer [currently Egress]. Ask the data subject to confirm receipt of the documents as soon as possible

6.1 Sharing personal data

We will not normally share personal data with anyone else without an appropriate lawful basis. However, there are circumstances where sharing may be necessary, including (but not limited to):

- where we need to liaise with other agencies to support a pupil or family
- where there is an issue that may put the safety of pupils or staff at risk
- where we must share data with local authorities, government bodies or law enforcement agencies to comply with legal obligations
- where we need to share data with emergency services to respond to an emergency situation
- where suppliers or contractors require data in order to provide services to the school (for example IT support, systems providers or specialist education services)

When sharing personal data with suppliers or contractors, we will:

- only share the minimum necessary information
- ensure there is an appropriate written agreement in place
- take reasonable steps to assure ourselves that the recipient will handle the data securely and lawfully

International transfers are subject to additional requirements and are covered in Section 10(International transfers).

7 Data subject rights

Data subjects have defined rights over the use of their data. These rights have been reinforced and extended by the UK GDPR and the Data Protection Act 2018.

These rights are:

- right to be informed
- right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision making and profiling.

The above rights are conditional depending on the reason we hold the data and why we may need to retain it.

7.1 Subject Access Requests (SARs)

Individuals have the right to request access to personal data that the school holds about them. Subject access requests can be made in any form. To help us respond efficiently, requests should include the individual's name and contact details and a clear description of the information requested.

If any member of staff receives a SAR (or a request that appears to be a SAR), they must forward it immediately to the DPO / Data Protection Lead.

We may ask for identification where necessary and may contact the requester to confirm the request.

7.2 Children and Subject Access Requests

Personal data about a child belongs to that child. Requests made by parents/carers for a child's personal data will be considered on a case-by-case basis. Where appropriate, we will consider the child's ability to understand their rights and the implications of the request, and whether the child has provided consent.

7.3 Responding to SARs and exemptions

We will respond without delay and within one month of receipt (or within one month of receiving any information needed to confirm identity). Where requests are complex or numerous, the response period may be extended in line with legal requirements. We will explain any extension within one month and set out the reasons.

We may withhold information where lawful exemptions apply, including where disclosure would adversely affect the rights of others, or where the information forms part of certain protected records.

Where a request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will explain our decision in writing and advise the requester of their right to complain to the ICO.

7.4 Other rights requests

Requests to exercise other data protection rights (such as rectification, erasure, restriction, objection, data portability, or rights relating to automated decision-making) should be submitted to the DPO / Data Protection Lead. Staff receiving such requests must forward them immediately.

Where we have a legal obligation to collect and process data or we are collecting the data to carry out a public task, we cannot always agree with any objection to the processing of data. We will consider all requests and explain the reason for the decision in writing.

Similarly, if an individual claims that there is an error in the recording of a child protection meeting or a behavioral incident, it is unlikely that these records will be amended because it is likely that the records contain the professional opinion of a social worker or other professional. Whilst the school would be unable to amend the original, we should place the individual's objections on file next to the original record so that their objections can be noted.

Where we rely on consent to process data about an individual, we will be obliged in most cases to apply the above rights.

When responding to data subject rights requests, the school will take a reasonable and proportionate approach, including when determining the scope of searches, the information to be provided, and whether a request may be considered manifestly unfounded or excessive.

8 Prohibited activities

The following activities are strictly prohibited when processing personal and special category data:

- Sharing passwords to access data
- Sending personal data to a personal email address to work on at home
- Sending data to unauthorised personnel. Always check that the recipients are authorised to view the information being sent. This includes those employed by the school who do not have authority to see that data.
- Sending personal data in an insecure format
- Leaving personal data unprotected
- Accessing information about a pupil, their family or a member of staff where there is no legitimate reason for doing so
- Accessing personal data about an individual for personal use
- Disclosing personal data to a recipient or third party outside of the school without a lawful basis
- Retaining personal data for longer than necessary without a lawful basis

Implications of breaching this policy

It is a condition of employment in the case of staff and contractors that they abide by the law and the policies of the school. Any breach of this policy could be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the school and/or the individual being held liable in law.

9 Privacy by Design

Under the Data Protection Act 2018 the school has a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. To achieve this, staff are expected to complete Data Privacy Impact Assessments to help identify and minimise any data protection risks, prior to any new processing.

Data Privacy impact assessments (DPIA)

The school must do a DPIA for any processing that is likely to result in a high risk to individuals' interests. It is good practice to do a DPIA for any major project which requires the processing of personal data.

Your DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

You should consult your Data Protection Officer who will need to approve the processing. You may need the assistance of any processors to explain how and where they process the data.

9.1 Artificial Intelligence (AI)

Artificial intelligence tools are increasingly accessible and may be used to support learning and workload where appropriate. However, AI tools can pose risks to personal and special category data.

Staff, pupils, parents/carers and contractors must not enter personal data or special category data into unauthorised AI tools or chatbots. Any such incident will be treated as a potential personal data breach and managed in line with Appendix A.

Before introducing any AI-based tool that may process personal data, staff must consult the DPO / Data Protection Lead and complete a DPIA where required. AI outputs must not be treated as fact and must be checked for accuracy and bias.

9.2 CCTV

The school may use CCTV to help maintain a safe environment. CCTV will be operated in a way that is lawful, proportionate and transparent. Clear signage will be displayed upon entry to the school to clearly state CCTV is in use.

Access to CCTV footage will be restricted to authorised staff. Requests for CCTV footage (including SAR-related requests) must be referred to the DSL/ DPO / Data Protection Lead.

CCTV footage will normally be retained for [28] days unless required for an investigation or where a lawful reason requires longer retention.

CCTV enquiries should be directed to: Indie King-Mand email: ikingmand@icknield.beds.sch.uk

9.3 Biometric recognition systems

Where the school uses biometric recognition systems (for example, fingerprint-based systems for catering or access), we will comply with applicable legal requirements.

Parents/carers will be informed before any biometric system is introduced for pupils, and written consent will be obtained from at least one parent/carer before the school first processes a pupil's biometric data.

Pupils and parents/carers may refuse or withdraw consent at any time. Where consent is withdrawn, the school will ensure biometric data is securely deleted and an alternative method is provided.

9.4 Photographs and videos

The school may take photographs and videos as part of school life (for example for displays, newsletters, school publications, the school website, and approved school communications). Where consent is required, we will obtain it in writing and will explain how images will be used.

Parents/carers and pupils should not share images or videos of other pupils publicly (including on social media) without appropriate consent, in order to safeguard children and respect privacy.

Consent for school use of photographs and videos may be refused or withdrawn at any time. Where consent is withdrawn, the school will take reasonable steps to stop further use and remove images from school-controlled platforms where practicable.

10 International transfers

Restricted transfers from the UK to other countries, including to the EEA, are now subject to transfer rules under the UK GDPR regime.

There are provisions which permit the transfer of personal data from UK to the EEA and to any countries which are now known as 'adequacy regulations'. There are also provisions which allow the continued use of any EU Standard Contractual Clauses ('SCCs'), both for existing restricted transfers and for new restricted transfers. A Transfer Impact Assessment is now available and is required to be completed if there is a transfer outside of the UK.

11 Conclusion

Compliance with the Data Protection Act 2018 is the responsibility of all members of staff and contractors. Any questions about this policy or any queries concerning data protection matters should be raised with the Head Teacher.

11.1 Training

All staff, contractors and governors will receive data protection training as part of induction and will complete refresher training as directed by the school. Additional training will be provided for staff who handle particularly sensitive information.

11.2 Monitoring arrangements

The school's leadership team and the Data Protection Lead/DPO are responsible for monitoring and reviewing this policy in practice. The policy will be reviewed on a scheduled basis and updated where necessary to reflect changes in law, guidance, or school processes.

11.3 Links with other policies and notices

This policy should be read alongside other relevant school policies and documents, including (where applicable):

- Acceptable Use / ICT and online safety policies
- Records retention arrangements
- CCTV policy
- Safeguarding policies and procedures (where personal data handling is relevant)
- Privacy notices for staff, pupils and parents/carers

12 Definitions

Subject Access Request or SAR	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be considered for disclosure, subject to applicable exemptions.
Freedom of Information Request or FOI.	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
Personal Data	Personal data means data which relate to a living individual who can be identified directly or indirectly from the data, particularly by reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Examples of personal data are the name and address of an individual; email and phone number; a Unique Pupil reference number or an NHS number
Special Category Data	Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Information relating to criminal activities or convictions is not special category data but must be treated with similar safeguards in place. Special category data includes:

	• race or ethnic origin of the data subject • their political opinions • their religious beliefs or other beliefs of a similar nature • whether they are a member of a trade union • their physical or mental health or condition • their sexual life • sexual orientation • Biometrics (where used for ID purposes) • Genetics
Data Controller	The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The School is the data controller of all personal data used and held by the school.
Data Processors	Organisations or individuals who process personal data on behalf of the data controller are known as data processors. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.
Data Subject	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
Lawful Basis	The grounds specified by the Regulations which need to be satisfied for any data processing to be legal. One ground needs to exist for processing personal data. Where special category data is processed a second ground must also exist.
Data Breach	A data breach is 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. A data breach may occur by accidentally sending an email to the wrong person or leaving a file in a public place. Breaches which result in a high risk to the individual must be reported to the ICO within 72 hours where required.
Staff	This includes any temporary members of staff and contracted staff, to include Governors and volunteers.

Appendix A: Personal Data Breach Procedure

1. Immediate action and reporting

1.1 Any staff member, contractor, governor or volunteer who discovers or suspects a personal data breach must report it immediately to the DPO / Data Protection Lead.

1.2 The person reporting the breach must provide all relevant details known at the time, including what happened, when, what data is involved, who may be affected, and what steps (if any) have already been taken.

2. Containment

2.1 The DPO / Data Protection Lead will take reasonable steps to contain the breach and minimise further risk. Actions may include:

- recalling emails (where possible)
- requesting recipients delete wrongly sent information and confirm deletion in writing
- isolating affected systems or accounts
- securing or recovering paper records or devices
- seeking support from IT providers where relevant

3. Assessment

3.1 The DPO / Data Protection Lead will investigate to determine whether a breach has occurred and assess:

- the type and sensitivity of data involved
- the number of individuals affected
- the likely consequences for individuals
- the likelihood and severity of harm
- what mitigations are possible

4. Notification and escalation

4.1 The DPO / Data Protection Lead will inform the Head Teacher and, where appropriate, the Chair of Governors.

4.2 The DPO / Data Protection Lead will decide whether the breach must be reported to the ICO and/or communicated to affected individuals, in line with legal requirements.

4.3 Where required, the ICO will be notified without undue delay and, where applicable, within 72 hours of the school becoming aware of the breach.

5. Communication with affected individuals

5.1 Where notification is required, we will communicate with affected individuals without undue delay and provide clear information about:

- what happened
- what data was involved (where appropriate)
- likely consequences

- steps taken or planned to address the breach
- advice on steps individuals can take to protect themselves
- how to contact the DPO / Data Protection Lead

6. Recording and learning lessons

6.1 The school will record all breaches (including near misses), regardless of whether they are reported to the ICO.

6.2 Records will include: the facts, causes, impacts, actions taken, and any follow-up steps.

6.3 The DPO / Data Protection Lead and relevant leaders will review incidents to identify trends and implement improvements (for example changes to processes, additional training, or technical measures).