Mayfield House
School

Data Protection Policy

Date policy last reviewed: 01 February 2026

Signed by:

Mike Williams	Headteacher	Date:	06 February 2026
Martyn Deakin	Director/Proprietor	Date:	06 February 2026

Signed on behalf of the Proprietors (Directors)

Last updated: Feb 2026

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. The right to be informed
9. The right of access
10. The right to rectification
11. The right to erasure
12. The right to restrict processing
13. The right to data portability
14. The right to object
15. Informing data subjects
16. Information right requests
17. Automated decision making and profiling
18. Data protection by design and default
19. Data Protection Impact Assessments (DPIAs)
20. Data breaches
21. Data security
22. Safeguarding
23. Publication of information
24. CCTV and photography
25. Cloud computing
26. Use of generative artificial intelligence (AI)
27. Data retention
28. DBS data
29. Monitoring and review

Statement of intent

Mayfield House School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK GDPR and the Data Protection Act 2018.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and directors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and **Mayfield House School** believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- The Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE 'Keeping children safe in education' (As amended)

1.2. This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2023) 'Data protection in schools'
- DfE (2025) 'Generative artificial intelligence (AI) in education'

This policy will be implemented in conjunction with the following other school policies:

- Photography and Images Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Surveillance and CCTV Policy
- Child Protection and Safeguarding Policy
- Records Management Policy

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
  - Racial or ethnic origin.
  - Political opinions.
  - Religious or philosophical beliefs.
  - Trade union membership.

- Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:
- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed 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.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. **Mayfield House School** will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR and DPA, and will provide comprehensive, clear and transparent privacy policies. The school will also provide evidence that it is complying with UK GDPR and DPA.

4.2. The school will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The school will also document other aspects of compliance with the UK GDPR and Data Protection Act where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

4.6. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.7. DPIAs will be used to identify and reduce data protection risks, where appropriate.

4.8. The Proprietors (Directors) are actively involved in the day-to-day oversight of the school and maintain regular on-site presence. Data protection compliance forms part of ongoing governance and operational oversight.

4.9. Weekly meetings are held between the Directors and senior leaders to review operational matters, including data protection, safeguarding and information-sharing practices. In addition, monthly governance meetings provide formal oversight, assurance and challenge in relation to data protection compliance, risk management and emerging issues.

4.10. This ensures that data protection arrangements are not only compliant on paper but are understood, monitored and embedded in practice across the school.

4.11. These arrangements are proportionate to the size of the school and reflect the high-risk, sensitive nature of the personal data processed within a specialist independent SEN setting.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws.

- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

5.2. The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.
- Providing annual training for all staff on the risks, limitations, and lawful processing requirements when using generative artificial intelligence (AI) technologies.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.4. The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

5.5. The DPO will report to the highest level of management at the school, which is the directors.

5.6. Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the UKGDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

6.3. The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

6.4. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.

— The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
— Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
— Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

6.5. The school will ensure that it has privacy notices established which clearly outline the reasons why it needs to collect personal data. The privacy notice will include the following explicit details:

- Why the school needs to collect personal data
- What the school plans to do with the personal data
- How long the school will keep the personal data
- Whether the school will share the personal data with any external organisations

6.6. The privacy notice will be clear and accessible to data subjects. The privacy notice will also be reviewed by the school's DPO at least annually and whenever significant changes are made to how the school processes the data that it collects.

6.7. The school will ensure that any parents, pupils and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which the school processes the data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.

- The right of the data subject to raise a complaint with the ICO in relation to any processing.

The school has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Pupils and their families
- School workforce
- Third parties
- Trustees and directors
- Volunteers

6.8. There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

6.9. Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in 7.7 and 7.8 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

6.10. The school may share information without consent in specific circumstances. To determine whether information can be shared without consent, the school will identify one of the other lawful bases for processing:

- **Contract** – the processing is necessary for a contract held between the school and individual, or because the individual has asked the school to take specific steps before entering into a contract.
- **Legal obligation** – the processing is necessary for the school to comply with the law (not including contractual obligations).
- **Vital interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

- **Legitimate interests** – the processing is necessary for the school's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.

6.11. Where the school is able to justify one of the lawful bases outlined in 6.2, an exemption applies, or there is a requirement under another law, information may be shared without consent.

6.12. Specifically, the GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

7. Consent

7.1. Consent must be a positive indication expressly confirmed **in words**. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

7.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7.2, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

7.8. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined in 7.2.

8. The right to be informed

8.1. Adults and children have the same right to be informed about how the school uses their data. The privacy notices supplied to individuals, including children,

in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

8.2. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period

The existence of the data subject's rights, including the right to:

- Withdraw consent at any time
- Lodge a complaint with a supervisory authority

- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

8.3. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

8.4. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided – this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed.

9.2. Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

9.3A. Where a parent or carer makes a SAR on a child's behalf, the school may request reasonable evidence of parental responsibility and, where appropriate, consider the child's competence and best interests before disclosure.

9.4. The school will verify the identity of the person making the request before any information is supplied.

9.5. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.

9.6. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.7. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.8. All fees will be based on the administrative cost of providing the information.

9.9. All requests will be responded to without delay and at the latest, within one month of receipt.

9.10. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.11. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.12. The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data the school will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

9.12A. The school may refuse or redact information where disclosure would reveal another individual's personal data without their consent, or where an exemption applies; in each case, reasons will be recorded and explained to the requester.

9.13. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received

10. The right to rectification

10.1. Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

10.6. The school will take reasonable steps to ensure that data is accurate or are rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data.

10.7. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

10.8. The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

10.9. Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

11.3. The school will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

11.4. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

11.5. The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

11.6. Requests for erasure will be handled free of charge; however, the school may impose a ‘reasonable fee’ to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

11.7. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.8. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.9. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question

12. The right to restrict processing

12.1. Individuals, including children, have the right to block or suppress the school's processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. Where the school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

12.6. The school will inform individuals when a restriction on processing has been lifted.

12.7. The school reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual

will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

13. The right to data portability

13.1. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The school will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

13.9. The school will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request

13.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy

14. The right to object

14.1. The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

14.4. Where personal data is processed for direct marketing purposes:

- The right to object is absolute and the school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The school will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

14.6. The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings.

14.7. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

14.8. The school will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive

14.9. Where no action is being taken in response to an objection, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. Informing data subjects

- The school ensures that pupils, parents and staff whose data is processed by the school are clearly and explicitly informed about how the school deals with their personal data. The privacy notice will outline the features and functions of the school's use of personal data, but the privacy notice itself must be easily accessible to all who wish to view it.
- The school will share its privacy notice with pupils:
- Through the pupils' induction pack when joining the school.
- At the start of each school year.
- On the school website.
- The school will share its privacy notice with staff through:
- Role application.
- Contract acceptation.
- Regular appraisal.
- The start of each school year.
- Staff notice boards and other relevant staff-centric space.

16. Information rights requests

- As well as the right to rectification, the school will recognise that its pupils have information rights, meaning that they have the right to access or amend any personal information that is held about them. The most common of these are SAR.
- A pupil can make an information rights request relating to any of the following:
- Changing any inaccurate information that the school holds about them
- Removing their personal information or record from the school's systems
- Restricting the school from processing any data held on the pupil
- Stopping the school from processing any personal data entirely
- The school will respond to any information rights request submitted verbally or in writing within one calendar month. If the case is deemed to be complex, then the school will extend the response deadline by an extra two calendar months.

- The school will ensure that staff are trained to recognise how to respond to information rights requests and how to differentiate between different types of information rights requests.

17. Automated decision making and profiling

17.1. The school will only conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

17.2. Automated decisions will not concern a child nor use special category personal data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

17.3. The school will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

17.4. The school will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

17.5. Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

17.6. The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

17.7. Generative AI systems will not be used to make solely automated decisions with significant effects on individuals, such as decisions regarding academic grading, behaviour sanctions, admissions, or staff appraisals, unless a suitably qualified person reviews and authorises the decision-making outcome.

17.8. When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.

- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

18. Data protection by design and default

18.1. The school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into all aspects of processing activities.

18.2. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

18.3. The school will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

19. Data Protection Impact Assessments (DPIAs)

19.1. DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

19.2. DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

19.3. A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency, and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

19.3A. For AI or cloud-based services involving personal data, the DPIA will confirm vendor assurances on data minimisation, storage location, sub-processors, retention/deletion, model-training opt-outs, and incident reporting.

19.3B. Deployment may proceed only where contractual terms (including a Data Processing Agreement) reflect the DPIA outcomes and provide enforceable safeguards.

19.4. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

19.5. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

19.6. A DPIA will be used for more than one project, where necessary.

19.7. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

19.8. The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

19.9. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

20. Data breaches

20.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

20.2. The **headteacher** will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their training.

20.3. Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

20.4. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

20.5. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

20.6. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

20.7. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

20.8. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

20.9. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

20.10. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

20.11. Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

20.12. Where notifying an individual about a breach to their personal data, the school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

20.13. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

20.14. The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the **Records Management Policy**.

20.15. The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

21. Data security

21.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

21.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

21.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

21.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

21.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

21.6. All electronic devices are password-protected to protect the information on the device in case of theft.

21.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

21.8. Staff and directors will not use their personal laptops or computers for school purposes.

21.9. All necessary members of staff are provided with their own secure login and password,

21.10. Password strength is enforced at system level and passwords are changed where compromise is suspected or required by system security settings.

21.11. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

21.12. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

21.13. When sending confidential information where legacy communication methods are used, staff will always check that the recipient is correct before sending.

21.14. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

21.15. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.

- Who will receive the data has been outlined in a privacy notice.

21.16. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

21.17. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

21.18. The school will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

21.19. The school takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

21.20. The **SBM** is responsible for continuity and for ensuring recovery measures are in place to ensure the security of protected data.

22. Safeguarding

22.1. The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

22.2. The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible.

22.3. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the **DSL** will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

22.4. The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.

22.5. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the **Child Protection and Safeguarding Policy**.

23. Publication of information

23.1. The school publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

23.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

23.3. The school will not publish any personal information, including photos, on its website without the permission of the affected individual.

23.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

23.5. The school's privacy notices (for pupils/families, staff, applicants and other groups) will be published on the website in an accessible location and updated when processing changes materially. Significant changes will be communicated directly to affected groups where practicable.

24. CCTV and photography

24.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

24.2. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and emails.

24.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

24.4. All CCTV footage will be kept for up to 20 days for security purposes; the **SBM** is responsible for keeping the records secure and allowing access. Any footage used for investigations will be kept for the duration of the investigation.

24.4A. The standard retention period of up to 20 days is based on a proportionate assessment of risk and operational need and is documented in the school's information asset and retention schedule.

24.4B. Where footage is required for a specific incident, investigation or legal process, relevant clips may be retained for as long as necessary for that purpose and will be securely flagged, access-controlled and reviewed regularly.

24.4C. Any extensions beyond the standard period will be recorded with the reason, decision-maker, review date and lawful basis.

24.5. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

24.6. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

24.7. Precautions, as outlined in the **Photography Policy**, are taken when publishing photographs of pupils, in print, video or on the school website.

24.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

25. Cloud Computing

25.1. For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

25.2. All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

25.3. If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, the school will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows the school to audit or verify compliance where necessary.

25.4. The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

25.5. All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

25.6. As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

25.7. The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

25.8. The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

26. Use of generative artificial intelligence (AI)

26.1. The school recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

26.2. Staff and pupils must not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

26.3. Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in school operations.

26.3A. Personal, identifiable or special category data will not be entered into any generative AI tool unless: (i) a DPIA has approved the specific use case; (ii) a compliant Data Processing Agreement is in place with the provider; and (iii) settings are configured to prevent the provider from retaining inputs for model training or unrelated analytics.

26.4. Use of generative AI tools must comply with the school's Acceptable Use Policy. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

26.5. Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the DPO and will be investigated in line with the school's data breach procedures.

27. Data retention

27.1. Data will not be kept for longer than is necessary.

27.2. Unrequired data will be deleted as soon as practicable.

27.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

27.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

28. DBS data

28.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

28.2. Data provided by the DBS will never be duplicated.

28.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

28.4. DBS certificates and certificate information will be retained for no longer than six months after the recruitment (or other relevant) decision, unless a longer period is strictly necessary and lawful; in all cases, storage will be secure, and access strictly limited.

29. Monitoring and review

29.1. This policy is reviewed annually by the DPO and the headteacher.

29.2. The next scheduled review date for this policy is February 2027.