Farmor's School
AN ACADEMY

Data Protection Policy

Author:	**Noelle Sturla**
Date of approval:	**April 2026**
Next Review Date:	**January 2028**
Review period:	**2 years**
Status:	**Statutory**

1 Statement of Intent

1.1 Farmor's School is legally required to keep and process certain information about its staff members, pupils, their families, governors, volunteers and external contractors in accordance with data protection legislation.

1.2 The school will, where necessary, share personal information with other organisations, including the Local Authority (LA), the Department for Education (DfE), other schools, educational bodies and children's services, where this is lawful, appropriate and necessary.

1.3 This policy sets out the school's approach to data protection and ensures that all staff and governors understand their responsibilities.

1.4 Farmor's School is committed to maintaining clear, practical policies supported by written procedures and regular staff training to ensure the secure and lawful processing of personal data.

2 Legal Framework

2.1 This policy has due regard to the latest versions of the following legislation and statutory guidance:

2.2 UK General Data Protection Regulation (UK GDPR)

- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended)
- Data Protection Act 2018 (DPA)
- Protection of Freedoms Act 2012
- The Data (Use and Access) Act 2025
- Working Together to Safeguard Children 2026
- Keeping Children Safe in Education

2.3 This policy also has regard to the following guidance:

- DfE Data Protection in Schools 2026
- IRMS Records Management Toolkit for Schools 2024

2.4 This policy operates in conjunction with the following school policies:

- Freedom of Information Publication Scheme
- Safeguarding Children Policy
- Online Safety Policy

3 Applicable Data

3.1 Personal data refers to information relating to an identifiable, living individual. This includes names, addresses and online identifiers such as IP addresses.

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

- 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.

3.3 Criminal offence data is subject to separate safeguards and may only be processed where authorised by law or where the school has official authority.

3.4 In accordance with the requirements outlined in the UK 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 UK 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.

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

4 Accountability

4.1 Farmor's School will implement appropriate technical and organisational measures to demonstrate compliance with the UK GDPR and DPA 2018.

4.2 The school will maintain records of processing activities, including:

- purposes of processing
- categories of individuals and data
- retention schedules
- data recipients
- security measures
- international transfers and safeguards

4.3 Additional documentation may include:

- privacy notices
- records of consent
- data sharing agreements
- Data Protection Impact Assessment (DPIA) reports
- data breach logs

4.4 The school will embed data protection by design and default into all processing activities, including:

- minimising data collection
- pseudonymising data where possible
- ensuring transparency
- enabling individuals to monitor processing
- improving security feature

5 Data Protection Officer (DPO)

5.1 Farmor's School has appointed a Data Protection Officer (DPO) who acts as the central point of contact for all data protection matters.

5.2 The DPO will advise the school on:

- compliance
- Data Protection Impact Assessments (DPIAs)
- audits
- training
- liaison with the Information Commissioner's Office (ICO)

5.3 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

5.4 The individual appointed as DPO will have professional experience and be highly knowledgeable about 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.

5.5 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.

5.6 The DPO will report to the highest level of management at the school, which is the governing board. The governing board must ensure that they involve the DPO in all data protection matters closely and in a timely manner.

6 Lawful Processing

6.1 The school will identify and document the lawful basis for processing before data is processed.

6.2 Personal data will be processed under one of the following bases:

- The consent of the data subject has been obtained.
- Processing is necessary for a contract held with the individual, or because they asked the school to take steps before entering 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 purpose of a recognised legitimate interest.
- 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 and the preceding condition are 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 with a basis in 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 with a basis in law
  - reasons of public interest in 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 a basis in law

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

6.6 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.

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

- Pupils and their families
- School workforce (including volunteers, contractors and trainees)
- Governors, members and trustees

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 section 6 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

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. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

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

7.3 The school ensures that consent mechanisms meet the standards of the UK 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. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.4 When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

7.5 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 above, 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. 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 above.

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 or 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:

- 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 (Subject Access Requests)

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

9.2 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. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information

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

9.4 Requests will be responded to within one month, with a possible two-month extension for complex cases.

9.5 Requests may be refused if manifestly unfounded or excessive.

9.6 The school will ensure that responding to a SAR does not disclose another individual's personal data unless:

- That individual consents, or
- It is reasonable to comply without consent

9.7 Where a large volume of data is held, the school may request clarification before responding.

10 The Right to Rectification

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

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

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

10.4 The school will take reasonable steps to ensure that data is accurate or is 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. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

10.5 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

10.6 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, have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2 The right to erasure applies where:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected or 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 erasure requests without undue delay and 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. 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. 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.

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

12.3 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.

12.4 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 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. 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.

13.2 Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

13.3 The school will provide the information free of charge.

13.4 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.

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

13.6 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

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. 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

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

- an individual's grounds for objecting must relate to their 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.

14.3 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.

14.4 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.

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

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. 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

14.7 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 Automated Decision-Making and Profiling

15.1 The school will only ever conduct solely automated decision making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract;
- authorised by law; and
- based on the individual's explicit consent,

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

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

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

15.4 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.

15.5 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 and
- it produces a legal effect or a similarly significant effect on the individual

15.6 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.

15.7 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;and
- securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

16 Data Protection by Design and Default

16.1 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. 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.

16.2 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;
- implementing basic technical measures within the school network and ICT systems to ensure data is kept secure;
- 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

17 Data Protection Impact Assessments (DPIAs)

17.1 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. 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. 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, and will be used for more than one project, where necessary.

17.2 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; and
- the use of CCTV.

17.3 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; and
- an outline of the risks to individuals..

17.4 The measures implemented in order to address risk:

- 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

18 Data Breaches

18.1 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. The headteacher will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training. All staff must report any actual or suspected data breach immediately to the DPO

18.2 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.

18.3 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.

18.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. 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. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.5 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;
- aa description of the proposed measures to be taken to deal with the personal data breach; and
- where appropriate, a description of the measures taken to mitigate any possible adverse effects,

18.6 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.

18.7 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.

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

18.9 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.

19 Data Security

19.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

19.2 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up and stored securely. Where digital data is saved on removable storage or a portable device, the device will be kept in a safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.3 Staff and Governors will use school email and Sharepoint for school purposes.. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.4 If staff need to use their personal laptops for school purposes, particularly if they are working from home, they will bring their device into school before using it for work to ensure the appropriate software can be downloaded and information encrypted.

19.5 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending.

19.6 Before sharing data, all staff will ensure:

- they are allowed to share it;
- that adequate security is in place to protect it; and
- who will receive the data has been outlined in a privacy notice.

19.7 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 responsibility for the data's security.

19.8 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are always supervised.

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

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

19.11 The school takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The School Business Manager (SBM) is responsible for the continuity and recovery measures which are in place to ensure the security of protected data.

19.12 When disposing of data, paper documents will be shredded, and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance.

19.13 The school holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

20 Safeguarding

20.1 The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe. Safeguarding takes precedence over data protection concerns.

20.2 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. 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; and
- the reason that consent has not been sought, where appropriate.

20.3 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. 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.

21 Publication of Information

21.1 The school publishes our Freedom of Information Publication scheme on the website outlining classes of information that will be made routinely available, including:

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

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

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

22 CCTV and Photography

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

22.2 The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for thirty days for security purposes; the SBM is responsible for keeping the records secure and allowing access.

22.3 Before the school is able to obtain the data of pupils or staff, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

22.4 The school will always indicate its intention of taking photographs of pupils and will receive permission before publishing them. If the school wishes to use images or 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. Precautions are taken when publishing photographs of pupils, in print, video or on the school website.

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

22.6 Parents and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

22.7 The school asks that parents and others do not post any images or videos which include any child other than their own child(ren) on any social media or otherwise publish those images or videos.

23 Data Retention

23.1 Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. 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. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained. Retention periods are based on the IRMS toolkit.

24 DBS Data

24.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. 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.

24.2 `The school processes Disclosure and Barring Service (DBS) data in accordance with the DPA 2018 and DBS Code of Practice.

24.3 DBS certificates will not be retained for longer than necessary.

24.4 The school will keep a record of:

- The date of the check.
- The certificate number.
- The type of check.
- The recruitment decision.

24.5 DBS information will be stored securely and accessed only by authorised staff.

25 Cyber Security

25.1 Appendix A sets out the cyber security controls and expectations that support the safe and lawful processing of personal data at Farmor's School

26 Monitoring and Review

26.1 This policy is reviewed every two years by the DPO. The next scheduled review date for this policy is April 2028

APPENDIX A — CYBER SECURITY STANDARDS (2026–2028)

Farmor's School Data Protection Policy

1. Purpose

This appendix sets out the cyber security controls and expectations that support the safe and lawful processing of personal data at Farmor's School. It complements the main Data Protection Policy and ensures the school maintains strong technical and organisational measures in line with UK GDPR, the DPA 2018, and the National Cyber Security Centre (NCSC) guidance for schools.

2. Scope

These standards apply to:

- All staff, governors, volunteers, contractors and trainees
- All devices used for school business (school-owned or personal, where permitted)
- All systems, platforms, and cloud services used by the school
- All personal data processed by the school

3. Core Cyber Security Principles

Farmor's School follows the NCSC's four pillars of cyber security:

1. **Secure configuration**
2. **Access control**
3. **Malware protection**
4. **Patch management**

These principles underpin all technical and organisational measures described below.

4. Passwords and Authentication

All staff must:

- Use **strong, unique passwords** for all school systems
- Enable **multi-factor authentication (MFA)** where available
- Never share passwords with anyone
- Never write passwords down or store them in unsecured locations
- Change passwords immediately if compromise is suspected

The school will:

- Enforce minimum password standards
- Require MFA for all administrative and remote-access accounts
- Monitor for unusual login activity

5. Device Security

School-owned devices

Staff must:

- Keep devices **locked** when unattended
- Use only **school-approved** devices for accessing personal data
- Ensure devices are **encrypted**
- Report lost or stolen devices immediately

The school will:

- Maintain up-to-date antivirus and endpoint protection
- Apply security patches promptly
- Restrict administrative privileges
- Monitor device compliance

Personal devices (BYOD)

Personal devices **must not** be used to store or transmit personal data unless explicitly authorised and protected by:

- Device encryption
- Secure passwords
- School-approved apps and platforms

6. Email and Communication Security

Staff must:

- Double-check recipients before sending emails
- Use **Bcc** for group communications
- Avoid sending sensitive data unless encrypted
- Never forward school data to personal email accounts
- Report suspicious emails immediately

The school will:

- Use email filtering and anti-phishing tools
- Provide staff training on phishing and social engineering
- Enforce secure email settings

7. Data Storage and Transfer

Staff must:

- Store data only on **school-approved systems**
- Never use personal cloud storage (e.g., personal Google Drive, Dropbox)
- Use encrypted USBs only where authorised
- Avoid transferring data unless necessary and lawful

The school will:

- Maintain secure cloud platforms with appropriate access controls
- Ensure data is encrypted in transit and at rest
- Review third-party processors for cyber security compliance

8. Network and System Security

The school will:

- Maintain secure firewalls and filtering systems
- Monitor network traffic for unusual activity
- Restrict access to systems based on job role
- Disable unused accounts promptly
- Conduct regular vulnerability assessments

Staff must:

- Only connect to secure, trusted networks
- Avoid using public Wi-Fi for school business unless using a VPN

9. Software and Updates

The school will:

- Apply security patches promptly
- Maintain an approved software list
- Block unauthorised software installations

Staff must:

- Never install unapproved software
- Ensure devices are updated regularly
- Report any system issues immediately

10. Cyber Incident Response

A cyber incident includes:

- Malware or ransomware
- Phishing attacks

- Unauthorised access
- System compromise
- Loss of data or devices

Staff must:

- Report incidents **immediately** to the DPO or IT lead
- Not attempt to investigate or fix the issue themselves
- Follow instructions from IT and the DPO

The school will:

- Contain and assess the incident
- Restore systems securely
- Notify the ICO within 72 hours if required
- Inform affected individuals where necessary
- Record all incidents in the Cyber Incident Log

11. Training and Awareness

All staff will receive:

- Annual cyber security training
- Phishing awareness and simulated exercises
- Updates on emerging threats
- Induction training for new staff

Governors will receive appropriate oversight training.

12. Third-Party Providers

Before using any third-party system, the school will:

- Assess cyber security controls
- Ensure data processing agreements are in place
- Confirm UK GDPR compliance
- Review the provider's incident response procedures

13. Remote Working

Staff must:

- Use school-approved devices where possible
- Access systems via secure connections
- Avoid printing personal data at home

- Store any temporary paper securely and dispose of it safely

14. Monitoring and Review

The school will:

- Review cyber security controls annually
- Conduct periodic audits
- Update this appendix in line with NCSC and DfE guidance
- Report cyber security risks to the governing board

15. Cyber Security for Exams and Assessment Systems

Farmor's School recognises that exam periods present heightened cyber security risks due to the volume of sensitive data processed, the use of awarding-body systems, and the statutory requirements set out by JCQ. This section outlines the controls in place to protect digital exam materials, online assessments, and exam-related personal data.

15.1 Scope

This section applies to:

- Exams Officers
- Senior Leaders
- IT staff
- Invigilators
- Teaching staff involved in NEA/coursework
- Any system used for exam administration or assessment

It covers:

- Digital exam papers
- Online assessment platforms
- A2C and awarding-body portals
- Candidate information
- Coursework and NEA evidence
- Secure storage and transmission of marks

15.2 Secure Access to Exam Systems

The school will ensure that:

- Access to awarding-body portals (e.g., AQA, Pearson, OCR, WJEC) is restricted to authorised staff only.
- Multi-factor authentication (MFA) is enabled wherever available.

- Passwords meet school security standards and are changed immediately if compromise is suspected.
- Accounts are disabled promptly when staff leave or change roles.
- Login activity is monitored for unusual or unauthorised access.

The Exams Officer and IT Manager will work together to ensure secure configuration of all exam-related systems.

15.3 Secure Handling of Digital Exam Materials

Where awarding bodies provide digital exam papers or materials:

- Files must be downloaded only on **encrypted, school-owned devices**.
- Files must be stored in **restricted-access, encrypted folders**.
- Printing must take place on **secure, school-approved printers** in controlled areas.
- Digital papers must **never** be emailed, transferred to personal devices, or stored on unapproved cloud services.
- Access logs must be retained for audit purposes.

Any breach or suspected compromise must be reported immediately to the DPO and Exams Officer.

15.4 Online Assessments and Computer-Based Exams

For online or computer-based assessments (e.g., Functional Skills, vocational qualifications, digital GCSEs):

The school will ensure:

- Devices are locked down to prevent access to other applications or the internet.
- Network stability and bandwidth are tested in advance.
- Invigilators are trained in digital exam protocols.
- Contingency devices are available in case of technical failure.
- Screens are positioned to prevent unauthorised viewing.
- Candidates cannot access personal accounts or files during the assessment.

The IT Manager will conduct pre-exam technical checks and provide on-site support during assessments.

15.5 Coursework and NEA (Non-Exam Assessment) Security

Digital coursework and NEA evidence must be:

- Stored on secure, access-controlled school systems.
- Never stored on personal devices or personal cloud accounts.
- Backed up regularly in line with school procedures.

- Shared only with authorised staff and examiners.
- Protected from accidental deletion or alteration.

Where video or audio evidence is required, staff must use **school-approved devices** and upload files promptly to secure storage.

15.6 Transmission of Marks and Candidate Data

When submitting marks, candidate information, or digital evidence:

- Submissions must be made only through awarding-body portals or secure upload systems.
- Files must be checked for malware before upload.
- Staff must verify the authenticity of any email claiming to be from an awarding body.
- Data must never be sent via personal email or unencrypted channels.

The Exams Officer is responsible for ensuring secure submission processes.

15.7 Cyber Incident Response During Exam Periods

A cyber incident affecting exams may include:

- System failure
- Ransomware or malware
- Loss of access to awarding-body portals
- Compromise of digital exam materials
- Network outage during online assessments

In the event of an incident:

1. **Report immediately** to the DPO, Exams Officer and IT Manager.
2. **Contain the issue** by isolating affected devices or systems.
3. **Activate contingency plans**, including paper backups or alternative devices.
4. **Notify awarding bodies** where required under JCQ regulations.
5. **Record the incident** in the Cyber Incident Log.
6. **Assess whether the ICO must be notified** (DPO decision).

The school will maintain a written **Exam Contingency Plan** in line with JCQ requirements.

15.8 Staff Responsibilities

Exams Officer

- Ensures secure handling of all exam materials.
- Manages access to exam systems.

- Works with IT to maintain system integrity.
- Reports incidents promptly.

IT Manager

- Ensures secure configuration of exam systems.
- Provides technical support during online assessments.
- Maintains logs and monitoring.
- Supports incident response.

Invigilators

- Follow digital exam protocols.
- Report any suspicious activity immediately.

Teaching Staff

- Store and handle NEA/coursework securely.
- Use only approved systems and devices.

15.9 Review

This section will be reviewed annually or following:

- JCQ updates
- Awarding-body changes
- Significant cyber incidents
- Changes to exam delivery methods (e.g., digital GCSEs)