Lunar Learning

Data Protection Policy

Last updated: February 2025

Next update: February 2026

1: Legal framework

This policy takes into account all applicable legislation and statutory guidance, 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*
- *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 (2024) 'Keeping children safe in education 2024'*

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 (2023) Generative artificial intelligence (AI) in education*

2: Applicable data

For the purposes of this policy, *'personal data'* refers to any information that can identify a living individual, including details such as online identifiers (e.g., IP addresses). The UK GDPR applies to both automated personal data and manual filing systems where personal data can be accessed based on specific criteria. It also applies to chronologically ordered data and pseudonymised data, such as key-coded data." '*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.*
  - *Principles.*

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, organisations 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.

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 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.

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

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, 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 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

3. Safeguarding

Lunar Learning recognises that the UK GDPR does not restrict or prevent the sharing of information when it is necessary to safeguard children. Lunar Learning is committed to ensuring that staff are aware of their responsibilities and are empowered to share personal information for safeguarding purposes. Concerns about sharing information should never impede the priority of safeguarding and protecting pupils.

Lunar Learning 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
- The reason that consent has not been sought, where appropriate

Lunar Learning will seek consent to share information where appropriate; however, staff will not attempt to gain consent if doing so would put a child at risk. The school will handle all instances of data sharing related to safeguarding a child in accordance with the Child Protection and Safeguarding Policy.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, Lunar learning would seek independent legal advice.

4. Data retention

Data will not be retained longer than necessary. Any data that is no longer required will be deleted as soon as possible. Certain educational records related to former pupils or employees may be kept for an extended period due to legal obligations or to facilitate the provision of references or academic transcripts. Paper documents will be shredded, and electronic records will be deleted and destroyed once they are no longer required.

5. Data breaches

The term ‘personal data breach’ refers to any security incident that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Lunar Learning will ensure that all staff are made aware of and understand what constitutes a data breach as part of their training.

Any notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the company becoming aware of the breach. If a breach is likely to pose a risk to the rights and freedoms of individuals, both the supervisory authority and the affected individuals will be notified directly. A 'high risk' breach means that the threshold for notifying the individuals is higher than for notifying the supervisory authority. The potential impact of the breach on individuals will be assessed on a case-by-case basis to determine whether it is necessary to notify the relevant supervisory authority. In cases where the breach is deemed sufficiently serious, the public will be informed without undue delay.

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
- 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

Where notifying an individual about a breach to their personal data, Lunar Learning 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.

Lunar Learning 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.

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

Lunar Learning 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.

6. Data security

Digital data is protected by passwords, both on local hard drives and network drives, which are regularly backed up. When digital data is stored on removable storage devices or portable devices, these devices will be kept in a locked filing cabinet, drawer, or safe when not in use. Memory sticks will only be used to store personal information if they are password-protected and fully encrypted. All electronic devices will be password-protected to safeguard the information in case of theft.

Confidential paper records will be stored in locked filing cabinets, drawers, or safes with restricted access, and will not be left unattended or in visible areas accessible to the public.

Circular emails to parents will be sent using blind carbon copy (bcc) to protect recipients' email addresses from being disclosed. Staff will always verify the recipient’s information before sending confidential data.