POLICY	**UK GDPR Data Protection Policy**
STATUS/DATE OF THIS VERSION	**January 2026**
APPROVED BY	**Board of Trustees**
RATIFIED BY	**Board of Trustees – January 2026**
REVIEW	**January 2027**

This policy is operated by all the schools in Unity Education Trust (as listed below).
There may be sections that are specific to one school and these will be added by the school either as an annex or in place of yellow highlighted sections below.

Any queries about the policy should be directed, in the first instance, to the Headteacher/Head of School:

- **Beeston Primary**
- **Garvestone Primary**
- **Grove House Infant**
- **Kings Park Infant**
- **Northgate High School and Dereham Sixth Form College**
- **The Pinetree School**
- **Churchill Park**
- **Greyfriars Primary**
- **Highgate Infant School**
- **Kings Oak Infant School**
- **Wimbotsham and Stow Primary**
- **Magdalen Primary**
- **St Germans Primary**
- **UET Compass Belton Academy**
- **UET Pathfinder Douglas Bader Academy**

If you would like to discuss anything in this policy, please contact:
Data Protection Officer: **Data Protection Education Ltd.**
Telephone: 0800 0862018
Email: dpo@dataprotection.education

Contents:

Statement of intent

Unity Education Trust and its member schools are required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

The Trust and/or its schools 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, trustees and governors 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 UET believes that it is good practice to keep clear practical policies, backed up by written procedures.

UET has overall responsibility for the policy. The Trust may delegate operational responsibilities to individual schools and, therefore, references below to "UET" or "the Trust" should be read as applying also to schools. Any parts of the policy which are school-specific are set out in appendix A.

1. Legal framework

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

- Data Use and Access Act 2025
- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the UK General Data Protection Regulation (UK GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the UK General Data Protection Regulation (UK GDPR) 12 steps to take now'

1.3. This policy will be implemented in conjunction with the following other Trust policies:

- **Freedom of Information Policy**
- **Records and Data Management Policy**
- **Data retention policy and schedule**
- **Information classification policy** and any other relevant policies.

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', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. 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.

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

4. Accountability

4.1. UET will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

4.2. The Trust will provide comprehensive, clear and transparent privacy policies. These are reviewed and updated annually and available on the Trust's website.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

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 Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.

- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.6. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO has been appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the Trust's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.3. The DPO will report to the highest levels of management which at the Trust is the CEO and at a school, which is the headteacher or head of school.

5.4. DPO for UET is; Data Protection Education Ltd. Registered office: 1 Saltmore Farm, New Inn Rd, Hinxworth, Baldock, SG7 5EZ.Telephone: 0800 0862018.

6. Lawful processing

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

6.2. The Trust will act as a data processor; however, this role may also be undertaken at the school level or by other third parties.

6.3. 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:
  - — Compliance with a legal obligation.
  - — The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - — For the performance of a contract with the data subject or to take steps to enter into a contract.
  - — Protecting the vital interests of a data subject or another person.
  - — 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 Trust in the performance of its tasks.)

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

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- 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).

7. Consent

7.1. Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

7.2. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

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

7.4. Where consent is given, a record will be kept documenting how and when consent was given.

7.5. The Trust 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.

7.6. 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.

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

7.8. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data,

7.9. Where there is concern that sharing the data would cause **'serious harm'.**

You can refuse requests for certain types of data if you believe they meet the 'serious harm' test, meaning that sharing the information would be likely to cause serious harm to the physical or mental health of any individual.

This applies to:

- Education data (i.e., personal data kept in educational records)
- Social work data

Similarly, you can refuse requests for child abuse data from anyone with parental responsibility for a pupil, if sharing the data would "not be in the best interests" of the child. This will cover any information as to whether a child is or has been the subject of child abuse, or may be at risk of it.

You should not share any health data via a request unless, within the last 6 months, you've been told by an appropriate health professional that the serious harm test is **not** met.

Even if you've been informed of this in the last 6 months, you must re-consult with the appropriate health professional about this if it would be reasonable for you to do so.

7.10 When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

8.2. If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3. 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 contact details of the controller (the Trust or the school), and where applicable, the controller's representative, as well as the DPO.
- The purpose of, and the legal 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.

8.4. 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.

8.5. 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.

8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7. In relation to data that is not obtained directly from the data subject, 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 have the right to obtain confirmation that their data is being processed.

9.2. Individuals 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. The Trust is committed to:

- Ensuring that individuals' rights to their own personal information can be appropriately exercised;
- Providing adequate training for staff to recognise and handle subject access requests;
- Ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to their own personal information;
- Ensuring that queries about individuals' rights to their own personal information are dealt with effectively and promptly;
- Being fair and transparent in dealing with a subject access request;
- Logging all subject access requests on the Trust's Data management system to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling processes and training requirements.

9.3. All staff are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy.

All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff within two working days.

For information and guidance on how the organisation will deal with a Subject Access Request see the Subject Access Request Procedure at Appendix 1

9.4. The Trust will verify the identity of the person making the request before any information is supplied. Where this is the case, the one calendar month deadline starts when the new information is received.

9.5. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

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

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

9.8. All requests will be responded to without delay and at the latest, within one calendar month of receipt; this timeframe includes weekends and school holiday periods; with no automatic extension for school closures. If the SAR cannot be processed due to school closure, tell the requester straight away why there's a delay (e.g., no staff access), how long it will be, and when they can expect a response. If you receive a request on the last day of the month and the following month is shorter, a response must be made by the last day of the shorter month.

9.9. 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. If possible, the requester should be informed if some data can be provided sooner.

9.10. Where a request is manifestly unfounded or excessive, the Trust 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.

9.11. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals 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 Trust will inform them of the rectification where possible.

10.3. Where appropriate, the Trust 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. Where no action is being taken in response to a request for rectification, the Trust 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 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 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
- 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

11.3. The Trust 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 exercise or defence of legal claims

11.4. 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.

11.5. 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.

11.6. Where personal data has been made public within an online environment, the Trust 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 have the right to block or suppress the Trust's processing of personal data.

12.2. In the event that processing is restricted, the Trust 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 Trust 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 Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust 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 Trust 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 Trust 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 Trust will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

13.1. Individuals 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:

- To personal data that an individual has provided 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 Trust 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 Trust 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 Trust will consider whether providing the information would prejudice the rights of any other individual.

13.9. The Trust 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 Trust 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 Trust will inform individuals 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 have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- 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 Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

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

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

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 Trust is not required to comply with an objection to the processing of the data.

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

15. Automated decision making and profiling

15.1. Individuals have the right not to be subject to a decision when:

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

15.2. The Trust 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.

15.3. When automatically processing personal data for profiling purposes, the Trust 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.

15.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

16. Privacy by design and privacy impact assessments

16.1. The Trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

16.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

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

16.4. 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.

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

16.6. 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.

16.7. The Trust 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

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

17. Data breaches

17.1. 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.

17.2. The Trust's CEO will ensure that mechanisms are in place for all staff members to be made aware of, and understand, what constitutes a data breach as part of their CPD training.

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

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

17.5. 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.

17.6. 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.

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

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

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

17.10. Within a breach notification, 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

17.11. 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. Data security

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

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

18.3. 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.

18.4. Where specific use cases require data to be saved on removable storage or portable devices, e.g., transferring exam answers, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

18.5. All other use of removable storage or portable devices is prohibited and server or online cloud-storage must be used as an alternative. Trust IT have measures in place to help staff retrieve data from removable storage or portable devices.

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

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

18.8. Staff, trustees and governors will not use their personal laptops or computers for school purposes unless they are password protected. Trustees and governors will be given a trust or school email address and all email communications will be via that email.

18.9. All necessary members of staff are provided with their own secure login and password, and where the systems allow, users will be prompted to change their password.

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

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

18.12. Staff should be aware of who is present when viewing their emails and private documents and should take extra precaution if the device is connected to an interactive whiteboard in the classroom so as not to share private information in the classroom environment.

18.13. When sending confidential information via email, staff will always check that the recipient is correct before sending to avoid data breaching due to human error.

18.14. 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 Trust's premises accepts full responsibility for the security of the data.

18.15. 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

18.15. 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.

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

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

18.18. The CEO will agree the appointment of person(s) responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Publication of information

19.1. The Trust 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

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

19.3. The Trust and its schools will not publish any personal information, including photos, on their website without the permission of the affected individual.

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

20.CCTV and photography

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

20.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

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

20.4. All CCTV footage will be kept for a short period for security purposes; the CEO will agree the appointment of person(s) responsible for keeping the records secure and allowing access.

20.5. The Trust will always indicate its intentions for taking photographs of pupils by means of image consent permissions and will only publish images in line with permissions given.

20.6. Similarly, if the Trust wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, image consent permission will be sought from the parent of the pupil.

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

21.Data retention

The Trust has a ratified Data Retention policy published and available on the website.

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

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

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

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

22.DBS data

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

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

22.3. 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.

23. Restricting use of unauthorised generative chatbots

Artificial Intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Copilot, and Gemini (formerly Google Bard). UET recognise that AI has many uses to help pupils learn and to support staff in data analysis, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into generative AI tools or chatbots.

If personal and/or sensitive data is entered into a generative AI chatbot, UET will treat this as a data breach, and follow the necessary procedures.

UET authorises the use of the following generative AI chatbots:

- Copilot (Microsoft)
- Gemini (Google)

UET may, on occasions, buy into services that have built in generative AI, such as; Management Information Systems, or Wellbeing tools. In these instances, UET will scrutinise the AI that is being used prior to authorisation. If at any point, UET deem any built-in generative AI to be a cause for concern, putting data at risk or generally unsafe, this will be communicated to staff without delay and communication with the service in question will commence, during which time, UET would request staff not to use the generative AI feature(s) until further notice.

24.Complaints and the Right to Challenge Data Use

Individuals may complain if they believe their data has been mishandled or their rights infringed.

Complaints can be submitted in writing, by email, or by phone.

Complaints will be handled in accordance with our UET Complaints Policy and acknowledged within 5 working days.

A substantive response will be provided within 1 calendar Month.

If dissatisfied, individuals may escalate to the Information Commissioner's Office and to the Data Rights Tribunal.

25.Policy review

This policy is reviewed on the date set down at the start of this document. We may change this policy at any time. Where appropriate, we will notify data subjects of those changes**.**

Appendix 1; SAR Procedure

Who can receive a SAR?

A SAR can be given to any staff member, contracted, permanent or otherwise. This procedure is applicable for all staff and managers:

- All staff are responsible for handling any information request received in line with UK GDPR requirements by following this procedure; and
- All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff and/or the Data Protection Officer within two working days.
- **Subject access request (SAR)** – is a request made by a data subject for information about, and access to, their personal data about themselves that The Organisation is processing.
- **Personal data** means any information relating to a living identified or identifiable natural person ('data subject'); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

How to recognise a valid Subject Access Request (SAR)

There is no formal way to submit a request. Valid SARs can be submitted in writing (e.g., letter, fax, email, website form, texts, Facebook, or Twitter) or verbally.

They include all requests for personal data, whether or not the data subject has referred to data protection, SARs, or the Data Protection Act and include requests which refer to Freedom of Information instead. It is up to you to recognise the request and deal with it as helpfully as possible.

Verbal requests are considered valid, but good practice suggests staff members receiving such requests, should record the details of the request and confirm the details with the requester in order to avoid later disputes.

Deadlines

Schools must deal with all reasonable requests within one calendar month, starting on the day the request is received. Variances to this may include:

- If an identity (ID) check or further information is required to comply with the request, then the deadline will be calculated from the date when the new information is received.
- If the request is deemed complex, the data subject should be informed of the decision, and the deadline may be extended by up to two months.

The data subject must also be informed as soon as possible if school holidays could impact the school's ability to carry out ID checks and/or meet the one calendar month deadline.

Key Points for Schools (Organisations)

- **One Month Rule:** The clock starts on the day you receive the request, even if it's a weekend or holiday; the deadline is the same calendar date next month (or the last day if no corresponding date).
- **No Automatic Extension:** School holidays don't get granted extra time; you must still meet the deadline.
- **Communicate Immediately:** If you can't process the SAR due to closures, tell the requester straight away why there's a delay, how long it will be, and when they can expect a response.
- **Complexity Extension:** If the request is complex (e.g., safeguarding records), you can extend the deadline by up to two months, but you must inform the requester of this within the first month.
- **Provide Partial Data:** If possible, release any easily accessible data within the initial month.

The SAR procedure

1. Request is received from a living Data Subject.
   Notify the responsible member of staff (the Headteacher). Do this without delay, and within **two working days** of receipt of the request.
2. Log the request on DPE Dashboard and inform the relevant people:

   - Record the request in the DPE Subject Access Request log:
     2..1. Log onto the Data Protection Knowledge Bank at: http://dataprotection.education
     2..2. Visit Logs>SAR Logs
     2..3. Select your school and click “Add”
     2..4. Add the known details in the form, including the date the SAR must be completed. Further details can be added later.
     2..5. Click the “Submit” button to save and log the SAR.
   - Updates from both the organisation and Data Protection Education should be added to the existing log online as they occur.

3. Acknowledge the SAR using template letter at Appendix 2
4. The responsible members of staff for dealing with SARs **qualify the request and confirms** the identity of the data subject.
   - If an ID check is needed, the one calendar month deadline starts when the new information is received. Usually in schools the requestor/parent/carer and their contact details and Parental responsibility will be known to you and where this is the case, this should be noted on the DPE form.

   - Adults should provide a photo ID plus another form of ID, this could be:

- their driving license or passport for the photo ID
- a utility bill or council tax bill that confirms their name and address
- If you need to clarify the request, send a letter seeking clarification and confirming the time to respond will be paused ('clock stopped') pending clarification. The one calendar month deadline starts from when the information is received.

5. If the identity/request is qualified, **evaluate the request** and compile the requested information:

- The time available under UK GDPR is **one month** to provide the information **free of charge** unless a request is complex, manifestly unfounded or excessive/repetitive.

6. ***IF*** requests are complex, manifestly unfounded or excessive, in particular, because they are repetitive, the DPO can decide to:

- For complex requests - extend the time by a further two months (while still notifying the data subject of this decision within one month). In these cases, the most senior level of the Trust should be consulted prior to informing the requester
- For excessive/repetitive/unfounded requests - charge a reasonable fee for administrative costs of providing the information; or providing a negative response to the request.

7. **Compile** and **send** the requested data.

- If the request was made electronically (digitally), you should provide the information in a commonly used electronic format.
- A requestor can ask for copies in a "permanent format" including paper.
- Where sending requests in the post, always double bag and send Special Delivery.
- Ensure the requestor is notified of their right to complain.

8. **Close** the request in the DPE Subject Access Request Log.

9. If a Complaint is subsequently received follow the Complaint's process; see policy on website.

10. members of the central Trust team are available to support with any queries.

Appendix 2; SAR acknowledgement template letter

[Headed paper]

[dated]

Dear [*insert name of individual making request*],

I am writing in response to your request dated [*insert date of request*]. I confirm that we have received your request and it is receiving our attention.

You will recall you asked for [*confirm what data subject right is being exercised and precisely what was requested, e.g., 'access to all records']*

[We will respond to your request within one month. ***OR***

Whilst we will endeavour to respond to your request within the usual one-month period, due to the [insert reasoning here e.g., complexity and size of your request] we may need to extend the period for responding in accordance with the UK General Data Protection Regulation.]

If you have any questions about this letter or your request, please do not hesitate to contact me, or our Data Protection Officer at dpo@dataprotection.education to discuss it further.

Yours sincerely,

[for and on behalf of

[*Insert name of school*]