DND Learning Trust

Durham and Newcastle Diocesan Learning Trust (DNDLT)
Company Number 10847279

Data Protection Policy

Every child matters and no child is ever left behind..."

"Let the little children come to me, and do not stop them;
for it is to such as these that the kingdom of God belongs."
Luke 18:15-17

Policy Reviewed and Adopted by Board of Directors: 20th May 2026, Interim Review 16th September 2026
Version: 10
Date of Next Review: Annual
Responsible Officer: COO

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. The right to be informed
9. The right of access
10. The right to rectification
11. The right to erasure
12. The right to restrict processing
13. The right to data portability
14. The right to object
15. Data Protection Complaints
16. Automated decision making and profiling
17. Privacy by design and privacy impact assessments
18. Data breaches
19. Data security
20. Publication of information
21. CCTV and photography
22. Data retention
23. EdTech procurement
24. Cloud computing
25. DBS data
26. Policy review

Vision Statement:

"Every child matters and no child is ever left behind"

Let the children come to me, and do not stop them; for it is to such as these that the kingdom of God belongs.

Luke +

At the DNDLT we believe everyone in our Trust is a child of God, adults and children alike. Every individual and every school matters, all are valued and celebrated, and no one should be left behind.

As a Diocesan Trust of the Dioceses of Newcastle and Durham we are here to serve children, and schools of all faiths and none. We welcome both Church of England and Community Schools to join us to serve our communities in the North East of England as part of our Trust family whilst remaining unique and distinct within their local context.

The Durham and Newcastle Diocesan Learning Trust is a place where we strive for the best outcomes for our children and staff. We work hard to achieve equity and flourishing for everyone. We want our staff and children to feel valued and celebrated given the opportunity to innovate and reach their full potential. We want our schools to be at the heart of their communities serving them in the way they know best, knowing they will be supported, encouraged and affirmed by a dedicated and specialist team.

Statement of intent

DNDLT is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the data protection legislation.

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

This policy is in place to ensure all staff, directors and academy councillors 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 **DNDLT** believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

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

- The Data Protection Act 2018
- The UK General Data Protection Regulation (GDPR)
- The Data (Use and Access) Act 2025
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- Protection of Freedoms Act
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE 'Keeping children safe in education'

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

- ICO 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE 'Data protection in schools'
- DfE Generative artificial intelligence (AI) in education
- DfE 'The Data Use and Access Act 2025'
- ICO 'Data (Use and Access) Act 2025' guidance

- DfE Generative AI: product safety standards

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

- Cyber-security Policy
- Freedom of Information Policy
- CCTV Policy
- Child Protection and Safeguarding Policy
- Safe use of AI Policy
- Data Retention Policy

2. Applicable data

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

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

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

2.3 'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

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

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of

the data subject in connection with employment, social security, social protection, health or social care purposes, public health and research.

3. Principles

3.1. In accordance with the requirements outlined in the 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. DNDLT will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR and DPA as amended.

4.2. The school will provide comprehensive, clear and transparent privacy policies. The trust will be able to demonstrate how data is processed as a whole across the MAT, and will take steps to ensure each individual school within the trust is adhering to the same procedure and that this is being

implemented and enforced in line with the wider trust policies. Internal records of school processing activities will be maintained in school.

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 school 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 will be appointed in order to:

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

5.2. An existing employee of DNDLT 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. The current DPO is Liane Atkin (Chief Operating Officer), liane.atkin@durhamdmat.co.uk . Each school will have an individual who is responsible for data protection within the school (nominated person).

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law.

5.4. The DPO will report to the CEO. The nominated person will report to the highest level of management at the school, which is the **Headteacher**.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task. Staff will ensure they involve the DPO in all data protection matters in a timely manner.

6. Lawful processing

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

6.2. Under the 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 school in the performance of its tasks.)
  - A recognised legitimate interest specified in Annex 1 to the UK GDPR, namely responding to a request for disclosure for another organisation's public task or official function; national security, public security or defence; emergencies; preventing, detecting or investigating crime; or safeguarding vulnerable individuals.

6.3. 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 the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

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

6.4 For personal data to be processed fairly, data subjects must be made aware through the school privacy notices outlining the reasons why it needs to collect personal data. The privacy notices will include the following details:-

- 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 school and, if not satisfied with the ICO in relation to any processing.

6.5 The school and DNDLT have privacy notices for the following groups, which outline the information above that is specific to them:

- Staff including prospective employees
- Pupils and their families
- Academy Councillors
- Trustees
- Visitors to our website

6.6 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.

7. Consent

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

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

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

7.4. 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.

7.5. 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.

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

7.7. 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 compete a consent form.

7.8. Where a child is under the age of **13** the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards 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 school 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 identity and contact details of the controller (and where applicable, the controller's representative) and 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.
    - Raise a complaint with the school (through the processes in the Complaints Procedures)
    - If not satisfied with the complaint outcome, lodge a complaint with a supervisory authority (the ICO).
- 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.

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

9.4. The school will make a reasonable and proportionate search for the requested personal data. It is not required to undertake searches that would be unreasonable or disproportionate in light of the importance of providing access to the information.

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

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

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

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

9.9. All requests will be responded to without delay and at the latest, within one month of receipt. Where the school reasonably requires information to confirm the requester's identity, evidence that a third party is authorised to act, or payment of a permitted fee, the response period will begin when that information, evidence or fee is received.

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

9.11. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to request a review by the DPO and if they are not satisfied with this outcome to the supervisory authority and to a judicial remedy, within one month of the refusal.

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

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.

- Reject requests that cannot be fulfilled without disclosing another individual's personal data unless that individual consents or it is reasonable to comply without consent.

- Explain to the individual who made the SAR why their request could not be responded to in full.

9.13. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the

request is in relation to and the time limit for responding to the request will be paused until clarification from the individual is received.

9.14. The school's response will explain the individual's right to make a data protection complaint to the school and to complain to the ICO.

10. The right to rectification

10.1. Individuals 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.

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

10.7. 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 to request a review by the DPO and if they are not satisfied with this outcome, 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
- The personal data is processed in relation to the offer of information society services to a child

11.3. 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

11.4. 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 of services.

11.5. 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.

11.6. Requests for erasure will be managed 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. 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.

11.8. 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 have the right to block or suppress the school's processing of personal data.

12.2. 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

12.3. 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.

12.4. 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 to request a review by the DPO and if they are not satisfied with this outcome, 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 have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. 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

13.3. 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.

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

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

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

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

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

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

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

13.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to to request a review by the DPO and if they are not satisfied with this outcome, to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The school 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, recognised legitimate interests or the performance of a task in the public interest
- Processing used for 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, recognised legitimate interests or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate

grounds for the processing, which override the interests, rights and freedoms of the individual.

- The school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

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

- The 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 only retain enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

14.5. Where personal data is processed for research purposes:

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

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

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

14.8. 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 request a review by the DPO and if they are not satisfied with this outcome, to complain to the supervisory authority and to a judicial remedy.

15. Data Protection Complaints

15.1 A data protection complaint is an expression of concern that the school has infringed data protection legislation in the way it has collected, used, shared, stored, secured, retained or otherwise processed personal data, or in the way it has responded to an information rights request. The complainant does not need to use legal terminology, refer to legislation, or use a prescribed form in order to make a data protection complaint.

15.2 The school will provide clear and accessible ways to make a data protection complaint through the Trust Complaints procedures, including an electronic route. Current contact details and the electronic complaints route will be published and in relevant privacy notices. Complaints made verbally, in writing,

by email, through social media or through any other school channel will be accepted.

15.3 Staff who receive a data protection complaint will record it and refer it without delay to the DPO or the person responsible for coordinating the response. The school will make reasonable adjustments and provide age-appropriate support, where required, and will respond urgently where a complaint raises an immediate safeguarding or security risk.

15.4 The school will:

- Acknowledge receipt of the complaint in line with the Trust Complaints Procedures and in any event within 30 days.
- Begin making appropriate enquiries and taking appropriate steps to respond without undue delay; the investigation will not be postponed until the acknowledgement period has expired.
- Keep the complainant informed of the complaint's progress and explain any delay without undue delay.
- Communicate the outcome without undue delay, including the findings, any action taken or proposed, and the right to complain to the ICO.

15.5 Where the complainant's identity or a representative's authority is uncertain, the school will request only the information reasonably necessary to verify it and will do so promptly.

15.6 Where the data protection complaint forms part of a wider complaint, grievance or safeguarding matter, the data protection element will be handled under this section and will not be delayed unnecessarily by the wider process.

15.7 Where a complaint concerns processing carried out by a processor or joint controller, the school will coordinate with the relevant organisation under the applicable contract or arrangement while retaining responsibility for its own controller obligations.

15.8 The school will keep a proportionate record of the complaint, acknowledgement, enquiries, evidence, progress updates, outcome and remedial action in line with the Records Management Policy. The DPO will review recurring themes and trends to identify improvements.

15.9 Using the school's complaints process does not affect the individual's right to complain to the ICO or seek a judicial remedy.

16. Automated decision making and profiling

16.1. For the purposes of this policy, a decision is based solely on automated processing where there is no meaningful human involvement in taking the decision. A decision is significant where it produces a legal effect or a similarly significant effect on an individual.

16.2. The school will not make a significant decision based solely on automated processing unless it has identified and documented an appropriate lawful basis, the processing is necessary and proportionate, and the safeguards in this section are in place. Recognised legitimate interests will not be used as the lawful basis for such a decision.

16.3. The school will only ever conduct solely automated decision making with legal or similarly significant effects based entirely or partly on special category data if the decision is:

- Necessary for entering into or performance of a contract **and** meets the substantial public interest condition in Article 9 (2)(g) of the UK GDPR.
- Authorised by law **and** meets the substantial public interest condition in Article 9 (2)(g) of the UK GDPR
- Based on the individual's explicit consent.

16.4. The school will not use solely automated processing to make a significant decision about a child.

16.5. The school will conduct a DPIA for significant solely automated decision and will assess accuracy, fairness, bias, discrimination, security and the particular risks to children and other vulnerable individuals.

16.6. The school will ensure that safeguards are in place which:

- Provide the individual with information about the decision.
- Enable the individual to make representations about the decision.
- Enable the individual to obtain human intervention by the school.
- Enable the individual to contest the decision.

16.7. Any human review will be meaningful. The reviewer will be suitably qualified, will consider the relevant information independently, and will have authority to change or reject the automated outcome; a nominal approval will not be sufficient.

16.8. The school will not use generative AI or another automated system to determine academic grading, behaviour sanctions, admissions, safeguarding decisions or staff appraisals without meaningful human involvement.

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

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

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

17. Data Protection by design and default and Data Impact Assessments

17.1. 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 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.

17.2. Where the school provides an online service likely to be accessed by children, it will take account of children's higher protection matters when deciding which technical and organisational measures are appropriate. This includes how best to protect and support child users, the fact that children may be less aware of data protection risks, consequences and rights, and their differing needs at different ages and stages of development. The school will document how these matters have been considered when designing and operating the service.

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

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- 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.

17.4. Data protection impact assessments (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 be conducted prior to the implementation of any

generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse

17.5. 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.

17.6. 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.

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

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

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

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

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

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

18.3. 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.

18.4. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. Where the school faces a data security incident, the DPO must be informed and will 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.

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

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

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

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

18.9. 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

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

18.11. 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.

18.12. 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 discussion with the DPO.

18.13. The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by requiring further 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.

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

19.3. 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.

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

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

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

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

19.8. Staff, directors and academy councillors will not use their personal laptops or computers for school purposes.

19.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

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

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

19.12. When sending confidential information staff will always check that the recipient is correct before sending.

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

19.14. 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.

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

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

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

19.18. The school business manager (SBM) is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

19.19. 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 on the disposal of ICT assets.

19.20. 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

19.1 The DNDLT and the school understand that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

19.2 The school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The DNDLT will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.

- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

19.3 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

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

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.

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

21. Publication of information

21.1. The school publishes a Freedom of Information 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

21.2. Classes of information specified above are made available quickly and easily on request.

21.3. DNDLT or the school will not publish any personal information, including photos, on their websites without the permission of the affected individual.

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

22. CCTV and photography

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

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

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

22.4. CCTV footage will not be retained beyond the purpose for which it was collected. The school will ensure that CCTV footage is retained only as long as necessary and will be securely deleted when no longer required. As a general rule CCTV footage will be kept for a maximum of [30 days] for security purposes unless it is required to be retained for a longer period in relation to an incident, investigation or legal obligation; the **SBM** is responsible for keeping the records secure and allowing access.

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

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

22.7. Precautions are taken when publishing photographs of pupils, in print, video or on the school website.

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

22.9. 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.

22.10. 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. Procurement and management of educational technology

23.1 For the purposes of this policy, **"EdTech"** includes digital tools and systems used to support or deliver education, learning, communication, assessment, or school administration. Any EdTech tool that processes personal data will be assessed and approved before it is purchased, trialled or introduced. The DPO will be consulted from the earliest stage and throughout implementation. The DSL and ICT lead will also be involved where safeguarding, online safety, or security risks are relevant.

23.2 Before approving an EdTech tool, the school will establish and document:

- The educational purpose of the tool and the categories of personal data it will process, including whether special category data is involved.
- Why each category of data is necessary and proportionate, ensuring that optional data fields and non-core features that are not required are disabled by default.
- The lawful basis for each processing activity and, where relevant, the condition for processing special category data.
- How personal data will flow through the service, who will have access to it, where it will be stored or processed, and whether any international transfers will take place.
- Whether the school, supplier or any other party acts as a controller, joint controller, processor, or sub-processor for each part of the service.

- Whether the tool uses AI, profiling or automated decision-making and, where it does, whether the requirements in the 'Automated decision-making and profiling' and 'Use of generative artificial intelligence (AI)' sections of this policy are met along with the DNDLT Safe Use of AI Policy.

23.3 The school will undertake proportionate due diligence on the supplier and will require sufficient information to verify that the tool meets the school's data protection, security, and safeguarding requirements. This will include considering whether:

- Data protection by design and by default is built into the tool.
- Appropriate security measures are in place, including encryption, secure authentication, audit logging, and systems for detecting unusual or unauthorised activity, with suitable independent assurance where available.
- Pupil-facing services provide appropriate filtering, monitoring, moderation, and audit trails, and meet relevant age-appropriate design standards where the supplier acts as a controller or joint controller.
- The supplier can support the school in responding to information rights requests and data protection complaints, investigating incidents and demonstrating compliance.
- Where AI is used, the supplier can explain how outputs are moderated, whether personal data is used to train the model, how inaccuracies and bias are mitigated, and what controls and monitoring are available to the school.

23.4 Before personal data is shared, the school will ensure that a written contract or data processing agreement clearly allocates responsibilities and covers:

- The school's documented instructions, confidentiality requirements, and access by authorised supplier staff.
- Security measures, the use and approval of sub-processors, and any international transfer arrangements and safeguards.
- The supplier's breach notification timescales and assistance with investigation, mitigation, and reporting.
- Support for data subject rights and data protection complaints, and the school's ability to obtain, correct, restrict, erase or export data where required.
- Retention, return, and secure deletion requirements, including agreed arrangements for backups, caches, and archives.
- Audit, assurance, and compliance information required by the school.

23.5 When an approved tool is implemented, access will be limited to authorised users and only the data fields and features necessary for the agreed purpose will be enabled. Privacy notices and other information provided to pupils,

parents, staff, and other users will be updated where required, and users will receive appropriate instructions or training.

23.6 The school will monitor approved EdTech tools and suppliers at planned intervals and when changes or updates are proposed. Reviews will cover security, performance, processing activities, sub-processors, new features, and contractual compliance. Features that involve additional personal data will not be enabled automatically. Where processing changes, the school will reassess the lawful basis and risks and will update the DPIA, privacy notices, and other relevant policies or information as appropriate.

23.7 At the end of a contract or when changing supplier, the school will follow an agreed exit plan. Personal data will be securely returned or transferred within agreed timescales, access will be revoked, and any remaining copies held by the supplier, including backups, caches, and archives, will be securely deleted. The school will obtain confirmation of deletion and retain an appropriate record of the completed exit process.

23.8 The school will not procure or continue using an EdTech tool where the supplier cannot provide sufficient information, meet the school's requirements, or reduce identified risks to an acceptable level.

24.Cloud computing

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

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

26.3 If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees and pupils will be removed when they leave the school and schools must notify One IT of leavers within a week of departure to ensure accounts are removed.

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

26.5 As with files on school devices, only authorised parties will be able to access files on the cloud. Only authorised parties will be able to access files on the cloud or Trust servers. An audit process is in place to alert the school should unauthorised access, deletion or modification occur (when the deletion / modification is deemed "unusual" by Microsoft's automated reporting systems). At any time, an audit can be run to look at any and all actions taken against data by an individual or against a file / folder. The auditing and automated detection systems ensure ongoing compliance with the school's policies for the use of cloud computing, all logs are immutable and cannot be modified or deleted.

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

24.7 One IT, the DNDLT IT support providers have ISO 27001 Information Security Management certification ensuring robust procedures and processes are in place.

25. Use of generative artificial intelligence (AI)

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

25.2 Generative AI tools used by the school will comply with data protection legislation and the school will ensure that providers meet the DfE's 'Generative AI: product safety standards'.

25.3 To protect data when using generative AI tools, staff members and pupils will:

- Seek advice from the DPO or ICT lead as appropriate.
- Check the type of tool being used is approved by the school.
- Understand how the tool uses personal data and whether this adheres to this policy.
- Acknowledge or reference the use of generative AI in their work.
- Fact-check results to make sure the information is accurate.

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

25.5 If personal data is entered into an AI tool, the person doing this will first check with the DPO or ICT lead that it is safe and appropriate to do so. To avoid a data breach, personal data will be protected within the tool and not used to further train the AI.

25.6 Use of generative AI tools must comply with the school's IT and Communications policy in the Staff Handbook. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

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

25.8 Further detail on the use of generative AI tools will be outlined in the Safe use of AI Policy.

26. Data retention

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

26.2 Unrequired data will be deleted as soon as practicable.

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

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

27. DBS data

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.

Policy review

This policy is reviewed annually by the **Chief Operating Officer of the DNDLT and Trust board**.

The next scheduled review date for this policy is **May 2027**.