

Policy

Data Protection

Approved by:	Board of Trustees
Date:	Summer 2026
Review Date:	Summer 2027 (or when legislation changes)
This policy applies to:	 DURHAM SIXTH FORM CENTRE

Contents

1. Policy Introduction and Purpose Statement	2
2. Legislation and Guidance	2
3. Definitions	2
4. The Data Controller	3
5. Roles and Responsibilities	3
Trust Board	3
Data Protection Officer	3
Principal	3
Chief Executive Officer	3
All staff	4
6. Data Protection Principles	4
7. Collecting Personal Data	4
Lawfulness, fairness and transparency	4
Limitation, minimisation and accuracy	5
8. Sharing Personal Data	6
9. Subject Access Requests and Other Rights of Individuals	6
Subject Access Requests	6
Students and Subject Access Requests	7
Responding to Subject Access Requests	7
Other data protection rights of the individual	7
10. Parental Requests to see the Educational Record	8
11. Photographs and Videos	8
12. Artificial Intelligence (AI)	9
13. Data Protection by Design and Default	9
14. Data Security and Storage of Records	9
15. Disposal of Records	10
16. Personal Data Breaches	10
18. Training	10
19. Monitoring Arrangements	11
20. Appendix A: Personal Data Breach Procedure	12
21. Appendix B: Actions to Minimise the Impact of Data Breaches	14

Links with other policies:

This Policy is linked to the:

- Freedom of information publication scheme
- Privacy Notices
- Online Safety
- Acceptable Use of ICT Statement
- Appropriate Data Processing Policy
- Complaints Procedure
- Data Retention and Deletion Policy
- Safeguarding (Child Protection Policy)
- Use of Photographic Devices and Images Statement

1. Policy Introduction and Purpose Statement

- 1.1. Our Trust aims to ensure that all personal data collected about staff, students, parents/carers, Governors, Trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
- 1.2. This Policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

- 2.1. This Policy meets the requirements of the:
 - UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
 - [Data Protection Act 2018 \(DPA 2018\)](#)
 - [Data \(Use and Access\) Act 2025](#)
- 2.2. It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence \(AI\) in education](#).
- 2.3. In addition, this Policy complies with our Funding Agreement and Articles of Association.

3. Definitions

Term	Definition
3.1. Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials). • Identification number. • Location data. • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
3.2. Special categories personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Genetics. • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes. • Health – physical or mental. • Sex life or sexual orientation.
3.3. Processing	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual, and also includes transmitting or transferring

	personal data to third parties.
3.4. Data subject	The identified or identifiable individual whose personal data is held or processed.
3.5. Data controller	A person or organisation that determines the purposes and the means of processing personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.
3.6. Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
3.7. Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

- 4.1. Our Trust processes personal data relating to parents/carers, students, staff, Governors, Trustees, visitors and others and therefore is a data controller.
- 4.2. The Trust is registered and has paid its data protection fee to the ICO, as legally required.

5. Roles and Responsibilities

- 5.1. This Policy applies to all staff employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this Policy may face disciplinary action.

Trust Board

- 5.2. The Trust Board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

Data Protection Officer

- 5.3. The Data Protection Officer (DPO) is responsible for overseeing the implementation of this Policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable. This is monitored by our Chief Operations and Finance Officer (COFO).
- 5.4. Trustees receive an update via the half termly CEO's Report and termly Principal's Report, or sooner if necessary, on data protection and GDPR compliance. This includes subject access requests, freedom of information requests and data breaches.
- 5.5. The DPO is the first point of contact for individuals whose data the Trust processes, and for the ICO.
- 5.6. Our DPO is contactable via dpo@durhamsixthformcentre.org.uk. Please contact the DPO with any questions about the operation of this data protection policy or the UK GDPR, or if you have any concerns that this data protection policy is not being or has not been followed.

Principal

- 5.7. The Principal acts as the representative of the data controller on a day-to-day basis.

Chief Executive Officer

- 5.8. Where the issue/practice relates to the work of the Trust central staff, the CEO acts as the representative of the data controller.

All staff

5.9. Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this Policy.
- Informing the Trust of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
 - with any questions about the operation of this Policy, data protection law, retaining personal data or keeping personal data secure;
 - if they have any concerns that this Policy is not being followed;
 - if they are unsure whether or not they have a lawful basis to use personal data in a particular way;
 - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
 - if there has been a data breach;
 - whenever they are engaging in a new activity that may affect the privacy rights of individuals;
 - if they need help with any contracts or sharing personal data with third parties.

6. Data Protection Principles

6.1. The UK GDPR is based on data protection principles that our Trust must comply with.

6.2. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).
- Collected for specified, explicit and legitimate purposes (purpose limitation).
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation).
- Accurate and, where necessary, kept up to date (accuracy).
- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation).
- Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality).
- Not transferred to another country without appropriate safeguards in place (transfer limitation).
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests).

6.3. Article 5(2) of the UK GDPR states that the controller shall be responsible for, and able to demonstrate, compliance with the principles (accountability). This Policy sets out how the Trust aims to comply with these principles.

7. Collecting Personal Data

Lawfulness, fairness and transparency

7.1. We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life.
- The data needs to be processed so that the Trust, as a public authority, can **perform a task in the public interest or exercise its official authority**.
- The data needs to be processed for the **legitimate interests** of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.

- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**.
- 7.2. For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:
- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**.
 - The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**.
 - The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
 - The data has already been made **manifestly public** by the individual.
 - The data needs to be processed for the establishment, exercise or defence of **legal claims**.
 - The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
 - The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
 - The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
 - The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.
- 7.3. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:
- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**.
 - The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
 - The data has already been made **manifestly public** by the individual.
 - The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
 - The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- 7.4. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
- 7.5. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

- 7.6. We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- 7.7. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
- 7.8. Staff must only process personal data where it is necessary in order to do their jobs.
- 7.9. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- 7.10. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with guidance from the Information and Records

Management Society (IRMS) and [the Records Management Toolkit for Schools and Academies](#). For further details, please see the 'Data Retention and Deletion Policy'.

8. Sharing Personal Data

- 8.1. We adhere to guidance outlined in [Keeping Children Safe in Education](#) and to advice in the DfE's [Information Sharing](#) which states: Data protection legislation (the Data Protection Act 2018 (the DPA 2018) and UK General Data Protection Regulation (UK GDPR) does not prevent the sharing of information for the purposes of safeguarding children, when it is necessary, proportionate and justified to do so.
- 8.2. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. In addition to safeguarding situations as outlined above, these include, but are not limited to, situations where:
 - There is an issue with a student or parent/carer that puts the safety of our staff at risk.
 - We need to liaise with other agencies.
 - Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
 - only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law;
 - establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share;
 - only share data that the supplier or contractor needs to carry out their service.
- 8.3. We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- 8.4. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.
- 8.5. Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject Access Requests and Other Rights of Individuals

Subject Access Requests

- 9.1. Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:
 - Confirmation that their personal data is being processed.
 - Access to a copy of the data.
 - The purposes of the data processing.
 - The categories of personal data concerned.
 - Who the data has been, or will be, shared with.
 - How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
 - Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
 - The right to lodge a complaint with the ICO or another supervisory authority.
 - The source of the data, if not the individual.
 - Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
 - The safeguards provided if the data is being transferred internationally.
- 9.2. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
 - Name of individual.

- Correspondence address.
- Contact number and email address.
- Details of the information requested.

9.3. If staff receive a subject access request in any form they must immediately forward it to the DPO.

Students and Subject Access Requests

9.4. Personal data about students belongs to that student, and not the student's parents/carers. Students at Durham Sixth Form Centre are considered mature enough to understand their rights under the implications of a subject access request, in line with ICO guidance. Therefore, any application from a parent/carer will be discussed with the student first to ensure they give their consent.

Responding to Subject Access Requests

- 9.5. When responding to requests, we:
- May ask the individual to provide 2 forms of identification.
 - May contact the individual via phone to confirm the request was made.
 - Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
 - Will provide the information free of charge.
 - May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary (these timeframes continue to apply when the school is closed during holidays).
- 9.6. We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of the student or another individual.
 - Would reveal that the student is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the student's best interests.
 - Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
 - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.
- 9.7. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.
- 9.8. When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

- 9.9. In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:
- Withdraw their consent to processing at any time.
 - Receive certain information about the data controller's processing activities.
 - Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
 - Prevent use of their personal data for direct marketing.
 - Object to processing that has been justified on the basis of public interest, official authority or legitimate interests.
 - Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).

- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

9.10. Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental Requests to see the Educational Record

- 10.1. Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) usually within 15 school days of receipt of a written request.
- 10.2. If the request is for a copy of the educational record, the Trust may charge a fee to cover the cost of supplying it, however the fee must not exceed the cost of supply.
- 10.3. This right applies as long as the student concerned is aged under 18.
- 10.4. There are certain circumstances in which this right can be denied, such as if it is considered that releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Photographs and Videos

- 11.1. As part of our activities, we may take photographs and record images of individuals within our Trust.
- 11.2. We obtain written consent from parents/carers and from students via the Use of Photographic Devices and Images Statement at enrolment, seeking their agreement that we may use photographs and video footage in:
- Printed publicity or promotional literature for the school and Trust, including leaflets, posters, newsletters and other display material.
 - School and Trust websites and other social media sites.
 - Media and local press (such as newspaper articles, press releases and television filming).
- 11.3. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
- 11.4. Any photographs and videos taken by parents/carers at events for their own personal use are not covered by data protection legislation. However, we ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers and students have agreed to this.
- 11.5. Where a student or their parent/carer chooses not to sign the Agreement, it may be necessary for students to be excluded from certain activities as a result. Given the age of students whilst studying at the school, it is also an expectation that they too take responsibility in removing themselves from such activities.
- 11.6. See our Photography Use Agreement form for more information.

12. Artificial Intelligence (AI)

- 12.1. Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Our Trust recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data.
- 12.2. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.
- 12.3. If personal and/or sensitive data is entered into an unauthorised generative AI tool, we will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix A.

13. Data Protection by Design and Default

- 13.1. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
 - Only processing personal data that is necessary for each specific purpose of processing and always in line with the data protection principles set out in relevant data protection law.
 - Completing data protection impact assessments (DPIAs) where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies, (the DPO will advise on this process).
 - Integrating data protection into internal documents including this Policy, any related policies and privacy notices (available on our website and [here](#)).
 - Ensuring that members of staff complete training on data protection and GDPR annually and that this Policy, any related policies and any other data protection matters are also shared annually.
 - Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
 - Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
 - Maintaining records of our processing activities, including:
 - for the benefit of data subjects, making available the name and contact details of our Trust and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices).
 - for all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

14. Data Security and Storage of Records

- 14.1. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage. In particular:
- Paper-based records are kept in a secure place when not in use (papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access).
 - Portable electronic devices, such as laptops and hard drives that contain personal data are password protected and/or encrypted.
 - Minimum password length - 8 characters
 - Password must meet complexity requirements
 - Be at least six characters in length
 - Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)

- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, \$, #, %)
- Maximum password age - 90 days
- Enforce password history - remembers last 24 passwords, this means a password can not be reused if it matches the last 24.
- Staff, students, Governors and Trustees who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see the Online Safety Policy / Acceptable Use of ICT Statement).
- Governors and Trustees access Trust reports via a secure online platform which is password protected. If reports are shared outside of this platform, they are password protected and the password is shared in a separate email.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

15. Disposal of Records

- 15.1. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
- 15.2. For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal Data Breaches

- 16.1. The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.
- 16.2. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix A.
- 16.3. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a Trust context may include, but are not limited to:
- A non-anonymised dataset being published on a Trust website.
 - Safeguarding information being made available to an unauthorised person.
 - The theft of a Trust laptop containing non-encrypted personal data about students.

17. Complaints

- 17.1. We take any complaints about how we collect and use personal information very seriously.
- 17.2. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance by emailing dpo@durhamsixthformcentre.org.uk or by calling 0191 383 0708 and asking to speak to the Data Protection Officer.
- 17.3. For information about how to make a complaint, please see our Complaints Procedure, available on our website [here](#). If you need any support accessing the Complaints Procedure, please contact us as per the details above.

18. Training

- 18.1. All staff are provided with data protection and GDPR training as part of their induction process and complete annual refresher training.

- 18.2. The Chair of Governors and the Chair of Trustees are provided with data protection training.
- 18.3. Data protection will also form part of continuing professional development, where changes to legislation, guidance of the Trust's processes make it necessary.

19. Monitoring Arrangements

- 19.1. This Policy will be reviewed by the DPO and COFO annually (or sooner, if required).
- 19.2. The Trust Board has overall responsibility for approving the Policy.

APPROVED

20. Appendix A: Personal Data Breach Procedure

- 20.1. This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner's Office (ICO).
- 20.2. On finding or causing a breach or potential breach, the staff member, Governor, Trustee or data processor must immediately notify the Data Protection Officer (DPO) by dpo@durhamsixthformcentre.org.uk.
- 20.3. The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
- Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people.
- 20.4. Staff, Governors and Trustees will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- 20.5. If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal (or CEO if appropriate).
- 20.6. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).
- 20.7. The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- 20.8. The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#).
- 20.9. The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored internally on the Trust's software system.
- 20.10. Where the ICO must be notified, the DPO will do this via the ['report a breach'](#) page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Trust's awareness of the breach. As required, the DPO will set out:
- A description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned.
 - the categories and approximate number of personal data records concerned.
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- 20.11. If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as

possible.

- 20.12. Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
- A description, in clear and plain language, of the nature of the personal data breach.
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- 20.13. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- 20.14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- Facts and cause.
 - Effects.
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- 20.15. Records of all breaches will be stored in the Data Breach Log, stored on the Trust's software system.
- 20.16. The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- 20.17. The DPO and CEO will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the Trust to reduce risks of future breaches.

21. Appendix B: Actions to Minimise the Impact of Data Breaches

21.1. We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. In each case, the DPO will assess the nature of the breach to determine if affected individuals or the ICO must be notified.

21.2. Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to attempt to recall it from external recipients and remove it from the Trust's email system (retaining a copy if required as evidence).
- In any case where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

21.3. Unauthorised website publication

- In the event that confidential or sensitive personal data is mistakenly published on the school website or any public-facing digital platform, the school will immediately remove the webpage or document from public view.
- The IT department will take steps to request the removal of cached versions of the page from search engine indexes (e.g. Google cache).
- The DPO will assess the duration of the exposure and the nature of the data to determine if affected individuals or the ICO must be notified.

21.4. Inappropriate internal data sharing

- If sensitive data is shared internally or with staff or governance boards without appropriate anonymisation or authorisation, access to the shared files, drives, or physical documents will be restricted or recalled immediately.
- The DPO will issue a formal reminder to the recipients regarding confidentiality and data minimisation, requiring them to delete or destroy any unauthorised copies.
- Data sharing protocols for staff, governance board and committee meetings will be reviewed to ensure future data is appropriately aggregated or pseudonymised.

21.5. Physical security breaches and asset theft

- If physical data assets or device hardware are lost or stolen, the IT department will immediately attempt a remote wipe and revoke all network access credentials associated with the device.

- The IT department will apply an immediate password reset and session termination for all user accounts associated with the stolen asset (e.g., email, MIS, cloud storage) to block unauthorised access via saved passwords or session cookies.
- If physical hardcopy documents (such as student files or safeguarding reports) are stolen, the Trust will immediately assess who may have access, report the theft to the police, and attempt to identify and secure any remaining copies.
- The IT department will verify the encryption status of the stolen device. If full encryption was active and robust, the data would be classified as "unreadable," significantly lowering the risk profile of the breach.
- If unencrypted or sensitive data (such as financial or safeguarding records) is deemed compromised, the DPO will promptly notify the affected data subjects and advise them on protective measures.

21.6. Commitment to data protection and ongoing training

- The Trust is fully committed to holding, processing, and safeguarding all personal data in accordance with the highest standards of data protection legislation. We recognise that effective data security relies not only on robust technical systems but also on a vigilant and well-informed workforce. To maintain this commitment and minimise operational risk:
 - **Mandatory staff training:** All staff members receive regular, mandatory data protection and cyber security training appropriate to their role, ensuring they understand their responsibilities regarding data minimisation, secure handling, and prompt incident reporting.
 - **Governance board oversight:** Members of the governance boards undergo regular briefing and training to ensure effective oversight of the Trust's statutory obligations, risks, and data compliance frameworks.
 - **Continuous review:** Data protection practices, training modules, and breach-mitigation procedures are reviewed routinely and immediately following any security incident to foster a culture of continuous improvement and data privacy awareness across the entire Trust.

APPROVED



Providence Learning Partnership is a company limited by guarantee [Companies House Number: 11652271] and an exempt charity registered in England and Wales.