BOHUNT
EDUCATION TRUST

Data Protection Policy

Approved by: Audit and Risk Committee	Date: 2nd December 2025
Next review date:	Autumn Term 2027

Contents

1. Purpose of Policy

Bohunt Education Trust (the Trust) has introduced this Policy to provide the operational framework within which its ethos of Enjoy Respect Achieve is reflected in its implementation of the Data Protection Act 2018 and UK GDPR, and to ensure its legal duties and charitable purposes are met effectively.

The Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This Policy complies with and discharges the Trust's legal duties with respect to:

- Data Protection Act 2018
- 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
- Protection of Freedoms Act 2012 (with respect to biometric data)
- Surveillance Camera Code of Practice 2015 (with respect to use of CCTV in particular)
- Information Commissioner's Children's Code of Conduct 2020
- Human Rights Act
- Keeping Children Safe in Education 2023 (as updated annually)
- Working Together to Safeguard Children
- Data Protection in School updated Sept 2023 (DfE guidance to schools, non statutory)
- Information Sharing ; Advice for Practitioners (July 2018)

This policy also complies with our funding agreement and articles of association.

3. Definitions

Criminal Offence Data means personal data which is linked to criminal offences, or which is specifically used to learn something about an individual's criminal record or behaviour

Data controller means a person or organisation that determines the purposes and the means of processing personal data.

Data processor means a person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Data subject means the identified or identifiable individual whose personal data is held or processed.

Personal data means any information relating to an identified, or identifiable, living individual. This may include the individual's: name (including initials); unique pupil reference number or other

Identification number; location data (whether gathered by any member School directly or via any other processor such as educational software or app provider);

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Processing means anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

Processing can be automated or manual.

School Data Protection Contact (DPC) means the individual appointed by each Headteacher under Section 5.6 of this Policy

Special categories of personal data means personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin or family life; political opinions; religious or philosophical beliefs; trade union membership; genetics; biometrics such as fingerprints, retina and iris patterns), where used for identification purpose; Health – physical or mental; sex life or sexual orientation

Trust DP Team means DPO, Compliance Coordinator and School DPCs acting together.

4. Equalities Assessment Impact Statement

The Trust is committed to treating all people equally and with respect irrespective of their age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex, or sexual orientation. We are committed to eliminating discrimination and recognise children's diverse circumstances. We ensure that all children have the same protection, regardless of our duties under the Equality Act 2010. We have reviewed the effect of this policy on those who may face additional or different barriers to securing its benefits than the population as a whole and have identified the following:

- Young people under 18 as a group identified by the Information Commissioner's Office as a more vulnerable group in general;
- Young people under 18 whose special category data is collected, processed, shared and retained;
- Applicants to or employees paid and unpaid roles where special category data is collected, processed, shared and retained;
- Other individuals where special category data is collected, processed, shared and retained including adult households including family members of young people under 18 where required for the Trust to deliver its legal duties relating to the education, safeguarding and care of all students applying to or on a member School's roll.

5. Roles and Responsibilities

5.1. All Staff, Volunteers, Contractors

The safeguarding and protection of privacy of all personal information is the responsibility of all staff, volunteers, contractors, and all external organisations or individuals working on our behalf who come into contact with such information in the course of their role. Some staff, volunteers or contractors will handle more categories of personal information or special category personal information more routinely and regularly in their day to day operational activity. As a result, such specialist staff will have additional or different duties and obligations with respect to data protection than other staff, volunteers or contractors in general. Specialist staff are responsible for the safeguarding and protection of privacy of such additional or different personal information.

All staff (including casual staff), volunteers, external organisations and contractors (including agency staff) are responsible, in accordance with the level of responsibility and accountability appropriate to the delivery of their operational role for:

- Collecting, storing and processing any personal data in accordance with this policy and the legal duty to safeguard and protect the privacy of such personal data:
- Informing the school of any changes to their personal data, such as a change of address, or next of kin
- Contacting the DPO or School Data Protection Contact 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 review of any contracts or sharing personal data with third parties

This policy applies to all staff, volunteers, and contractors employed by the Trust directly or through any member School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.2. Trust Board

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations. The Trust is the data controller. The Trust is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5.3. CEO

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

5.4. Heads of Schools

The CEO may further delegate the right to act as the representative of the data controller to each Headteacher on a day to day basis in accordance with the Scheme of Delegation.

5.5. Local Governing Bodies

The Local Governing Bodies are responsible for ensuring that this policy is implemented in each School and that they hold the Headteacher, through annual reporting and other related activities, accountable for ensuring its provisions are delivered.

5.6. School DPCs

The School Data Protection Contacts:

- Act as the first point of contact within School for all queries and questions from colleagues and others around data protection and seek advice from the Trust DP Team as appropriate
- Act as the first point of contact within School for the Trust DP Team for all data protection queries, including to support the provision of information and other assistance upon request to the DPO for internal audit or other audits as required from time to time
- Ensure that all requests for information by data subjects are passed immediately to the Trust DP Team and support the DP Team to gather information for response to such requests within the required time frames to allow for DP Team review and compliance with legal timeframes
- Ensure that the School's data protection infrastructure is shared with the Trust DP Team
- Working with DP Team and at its direction if given, makes senior leaders in School aware that they must ensure:
    - that the school data map must be established, updated and reviewed regularly to ensure its currency and accuracy at any point in time
    - that there is a routine process by which personal information is destroyed when necessary in line with the Data Retention Schedule and other guidance
    - all BET provided data protection material (including consents for marketing upon new staff or student admission) is used
    - all BET provided data protection training at induction for all new joiners and for all existing staff and volunteers
    - all personal information shared outside of the Trust complies with the Data Sharing Principles
- Immediately report any data breaches within school to Trust DP Team using the shared data breach log and ensure any matter that requires escalation to the Trust DP Team in accordance with the Data Breach Escalation System is brought immediately to the Trust DP Team's attention
- Provide assistance to the Trust DP Team as requested in case of breaches reported to the Information Commissioner's Office
- Action all requests/briefings from the Trust DP Team across School and attend all training as established by the Trust DP Team

5.7. Data Protection Officer

The data protection officer (DPO) is responsible for advising on the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable as well as advising on appropriate training for all staff where requested. The DPO will work with the Compliance Coordinator to establish the DP Team and ensure regular briefings and training for School DPCs.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the Board their advice and recommendations on school data protection issues.

The DPO is also -via School DPCs- the first point of contact for individuals whose data the school processes, and for the ICO.

Details of the DPO are available from info@bohunttrust.com or via the Trust's website.

6. UK GDPR Principles

The UK GDPR is based on data protection principles that our Trust and all member schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

7. Collecting Personal Data

7.1. Lawfulness, fairness and transparency

7.1.1. Personal Data – collection, processing, retention, deletion, sharing

All staff, volunteers, contractors and the Trust as a whole will only collect, retain, process and share 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 school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school 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 school, 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 school (where the processing is not for any tasks the school 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 pupil) has freely given clear **consent**

7.1.2. Special Category personal data

For special categories of personal data, we will also meet one of the special category conditions for collecting, retaining and processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) 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

7.1.3. Criminal Offence Data

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 pupil) 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

7.2. Informing individuals prior to collection of any personal information

7.2.1. Privacy Notices

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. This is through reference to our Privacy Notices or other privacy notification if Privacy Notices do not apply.

7.2.2. Fairness

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.

7.2.3. Online services offered requiring consent

If a member School offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, it will obtain parental consent where the student is under 13

(except for online counselling and preventive services).

7.3. Limitation, minimisation and accuracy

7.3.1. Data Minimisation and transparency

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.

7.3.2. Change of use

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.

Staff, volunteers, contractors and any other external party engaged by the Trust or member School must only process personal data where it is necessary in order to do their jobs.

7.3.3. Accuracy

All member Schools and the Trust will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

7.3.4. Deletion

In addition, when staff, volunteers and contractors no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

8. Sharing personal data

8.1. General approach

The Trust will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- there is a concern or issue with a pupil or parent/carer or member of staff, volunteer or contractor that puts the safety of any student, member of staff or other members of our School community at risk
- a member of staff, volunteer or school needs to liaise with other agencies – we will seek consent as necessary before doing this where it will not risk harm or is otherwise not practicable or prevented by law
- a supplier or contractor needs data to enable Schools or the Trust to provide services to staff and pupils – for example, IT companies. When doing this, all members of staff 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
    - Follow the internal process for securing data protection risk assessment and logging on Trust data sharing agreement log

Schools may also share personal data with law enforcement and government bodies where we are legally required to do so, including sharing personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

8.2. International transfers

Where any member of staff undertakes to agree to transfer personal data internationally (i.e. outside of the four countries that make up the United Kingdom), they will do so in accordance with UK data protection law. Following the internal process for securing data protection risk assessment enables staff members to discharge this responsibility.

9. Subject access requests and other rights of individuals

9.1. Circumstances where a subject access request may be necessary, and where it is not necessary

9.1.1. Sharing personal information about students with parents as part of school's normal relationship with parents and parental rights under parental responsibility

In the vast majority of situations where a parent or student wishes to access personal information collected, held, processed, retained or shared by any member School or the Trust, it is very likely that that information has already been shared or is fully available in any event with the data subject and/or the parent.

Parents have rights outside of the UK GDPR and Data Protection Act 2018 to all information relevant to the education of their child, save in very limited circumstances where prevented by statutory legislation or act of court (such as court order) or where there is a risk of serious harm to any other individual in disclosing the information.

9.1.2. Information collected, processed and retained on students and parents/carers is visible to relevant data subject as normal matter of course

All BET Schools, staff, volunteers and contractors work to ensure that both students and parents have the same visibility of all information as staff. A successful relationship throughout a child's time in the School relies on such transparency and openness of information between parent, student and School. It is not in the School's interest to undermine the success of this relationship by collecting or retaining information that is not shared with the student or parents/carers.

Information around interventions and in school support, behaviour, attendance, homework and programmes of study are available to students as well as parents and carers on School systems such as Student or SEND passports; SIMs Lite; ClassCharts; Teams/Google classroom notifications to parents; Studybugs and School Comms (including termly reports). This personal information about students is visible to parents/carers outside of the UK GDPR regime.

9.1.3. Exceptions

There are some limited exceptions, Examples are:

- An exception will relate to the working information gathered throughout each term by all staff. During each term this working information is used to review progress by individual class teachers, subject leaders and other educational leaders in order to ensure the learning and teaching a student receives is adapted to their particular educational journey. Once the working information has been reviewed, it is used to provide termly reports and/or information shared at parent consultations and/or via other review mechanisms relating to

pastoral, welfare or SEND needs. Working information is then deleted once the reporting via School systems has been completed.

- Where sharing information is not permitted by law for any reason, including with respect to privacy of other third parties or where there is a risk of harm in sharing, or where a student shares information not relevant to their educational record and may request, initially, confidentiality. All such exceptions will be considered on a case by case basis, in the best interests of the student concerned. A subject access request will not guarantee disclosure where such an exception has been determined.

9.1.4. Provision of copies of material already provided

It can often be the case that less personal information about their child can be shared with parents/carers via a subject access request than via a request for copies of information already provided to parents in their capacity as parents with legal parental responsibility.

It is very rare that there will be additional personal information about a young person that has not already been shared with, or is visible via School systems, or been made known in other ways to parents and carers. Staff are always happy to provide copies of material previously provided and mislaid, within reason. This includes correspondence parents have had with school (which is not required to be provided to parents/carers under the subject access request regime). Schools will, where possible, assist with provision of mislaid information for parental records. Such requests must however be reasonable in time, content and cost to the School.

Where parents, students or staff are considering the need to make a subject access request, the Trust DP Team are always happy to advise if there is a quicker, more efficient way of obtaining the same information.

9.1.5. Staff personal information

Staff members can access copies of their personnel file by emailing hr@bohunt.hants.sch.uk. It is not the Trust's practice to expect further personal information about staff members to be collected, retained or processed other than via each individual member of staff's personnel file.

9.2 Subject access requests

Any individual may nevertheless wish to exercise the right to make a 'subject access request' to gain access to personal information that the school 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

9.3. Submission of Subject Access Request

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

If staff receive a subject access request in any form they must immediately forward it to the Trust DP Team.

9.4. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

9.4.1. Age of Consent

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.5. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone or face to face 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

9.6. Non disclosure

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 pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child'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

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.

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.

9.7. Other data protection rights of the individual

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
- 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)

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

10. Biometric recognition systems

10.1. Protection of Freedoms Act 2012

Where any member School or our contractors use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will ensure we and our contractors' comply with the requirements of the Protection of Freedoms Act 2012.

10.2. Consent

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it. Each child will also be requested to give consent.

For all pupils and students (regardless of key stage or age), if any pupil or student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

10.3. No requirement to grant consent

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Please contact your School DPC.

10.4. Withdrawal of consent

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted either by us or by any contractor.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

All member schools use CCTV in various locations around school sites to ensure it remains safe. As a Trust, we follow the ICO's guidance and Surveillance Camera Commissioner's Code of Practice for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School DPC or DPO.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

12.1. Year 6 and below

At admission, all member Schools will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

12.2. Year 7 and above

At admission, all member Schools will obtain written consent from parents/carers, or pupils aged 18 and over regarding each individual student, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within member school on notice boards and in member school or Trust magazines, brochures, newsletters, etc.
- Outside of member school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school or Trust website or social media pages

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.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no student or member of staff will be permitted to enter such personal information into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, this is a data breach, and will follow the personal data breach procedure outlined in appendix 1.

14. Data protection by design and default

The Trust 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 (see section 6)
- Completing data protection impact assessments where the Trust or member school'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)
- Where appropriate, having regard to the provisions of the ICO's Children's Code of Conduct and ensuring that apps, websites or games that a member School requires a student to share personal data with for the purposes of education comply with the 15 principles of the Code of Conduct. Each member School and the Trust recognises and is committed to the Code's aims, which are to ensure that young people have a baseline of protection automatically by design and default, so that they are protected within the digital

world rather than being protected from it. In the same way that young people are protected differently to adults in the real world, the Children's Code of Conduct ensures they are treated differently in the digital world too.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and where feasible with resources available 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 school Data protection Contacts, 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

15. Data security and storage of records

- Each member School and where applicable the Trust 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 and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office and where in hard copy, obtain the School DPC and Headteacher's express prior permission
- Passwords that are at least eight characters long containing letters, numbers and special characters are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students, volunteers, trustees and governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (and are expected to adhere to the BET Acceptable Use Policy)
- Where the Trust or School needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8). This will include a data protection impact assessment and a data

sharing agreement where necessary. Advice will be sought from the School Data Protection Contact or the DPO.

16. Disposal of records

- 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 the Trust or member School cannot or do not need to rectify or update it.
- For example, each member School and the Trust shreds paper-based records, and overwrites or deletes electronic files. A member School or the Trust may also use a third party to safely dispose of records . If a member School or the Trust does so, it will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

- Each member School and the Trust will make all reasonable endeavours to ensure that there are no personal data breaches.
- In the unlikely event of a suspected data breach, all staff, volunteers or third parties follow the procedure set out in the data breach process. Further information is available from the School Data Protection Contact or the DPO.
- When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:
    - A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
    - Safeguarding information being made available to an unauthorised person
    - The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff, volunteers, third parties providing services on behalf of the member School, Trustees and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's or member school's processes make it necessary.

19. Monitoring arrangements

- The Audit and Risk Committee is responsible for monitoring , reviewing and approving this policy, every three years
- The Committee will seek advice from Trust leaders directly, as well as the Data Protection Officer through the annual data protection reports
- Note: the DfE's latest guidance at November 2025 does not include data protection in its list of statutory policies for maintained schools or academies, including free schools, however it is a legal requirement that our school/trust has data protection policies and procedures in place and we as a Trust have opted to keep a data protection policy in place.

20. Links to other policies

This policy links to the following Trust policies:

- Safeguarding and Child Protection policy

- Acceptable Use Policy
- Staff and trustee/governor Code of Conduct
- Freedom of Information Publication Document
- Privacy Notices
- Procurement Policy