BETTER TOGETHER LEARNING TRUST

DATA PROTECTION POLICY

STATUTORY POLICY

Document Reference:	S11
Date of Approval:	October 2022
Approved by:	Board of Directors
Version No:	V. 1
Last Review Date	October 2022
Next Review Date:	October 2024
Policy Owner:	Network Manager/Chief Operations Officer
Document History:	Version 1: September 2021

Glossary

The term **'School'** is used as standard to mean the educational establishment that is adopting this policy.

The term '**Headteacher'** is used to refer to the person with overall day-to-day responsibility of the **School.**

Directors are the Trustees of the Board.

LGB is the Local Governing Body.

Our Trust aims to ensure that all personal data collected about staff, students, parents, trustees, members, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format and also meets the requirements of the GDPR and the expected provisions of the DPA 2018. Guidance from the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational records.

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

The Data Controller

The Trust processes personal data relating to parents, students, staff, members, trustees, governors, visitors and others and therefore is a *data controller*.

Roles and Responsibilities

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.

1. **The board:** The board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.
2. **Data protection officer:** 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. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the Trust/Academy/School processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is the Chief Operating Officer and is contactable using the following mechanisms **Telephone- 01933** 304957 sdownhill@friars.northants.sch.u**k or Friars Academy, Friars Close, Wellingborough, NN8 2LA**.

3. **Executive Head Teacher:** The Executive Head Teacher/Head Teacher/Head of School acts as the representative of the data controller on a day-to-day basis.
4. **All staff:** Staff are responsible for collecting, storing and processing any personal data in accordance with this policy; informing the Trust/Academy/School of any changes to their personal data (such as change of address); contacting the DPO with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure and also if they have concerns that this policy is not being followed. If staff are unsure whether or not they have a lawful basis to use personal data in a particular way or 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 of the European Economic Area, they should again contact the DPO.

Data protection principles

The GDPR is based on data protection principles that the Trust must comply with and these principles state that personal data must be:

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

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

Collecting personal data

Lawfulness, fairness and transparency

The Trust will only process personal data where it has one of six '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 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 (an example of this would be to protect life)
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school 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**

For special categories of personal data, the Trust will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If the Trust offer online services to students, such as classroom apps, and the Trust intends to rely on consent as a basis for processing, the Trust will obtain parental consent (except in the case of online counselling and preventive services). Whenever the Trust first collects personal data directly from

individuals, the Trust will provide those individuals with the relevant information required by data protection law.

Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. The Trust will explain these reasons to individuals when data is first collected. If the Trust would like to use the collected data for reasons other than those given when first collected, the Trust will inform the individuals concerned beforehand, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to carry out their jobs.

When staff no longer need the personal data they hold, they must ensure that it is deleted or anonymised. This should be done in accordance with the Trust's record retention schedule.

Sharing personal data

The Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of staff within the Trust at risk
- When the Trust needs to liaise with other agencies – in this case the Trust will seek consent as necessary before doing this
- Suppliers or contractors need data to enable the Trust to provide services to staff and students (for example, IT contractors/installers). When doing this the Trust will only appoint suppliers and contractors that can provide sufficient guarantees that they comply with data protection law; establish a data sharing agreement with the supplier or contractor, either in contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the Trust shares. The Trust will only share such data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

The Trust will also share personal data with the Police or other government bodies where the Trust has a legal duty to do so, including:

- The prevention or detection of a crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy safeguarding obligations
- Research and statistical purposes, so long as personal data is sufficiently anonymised or consent has been provided

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects students and/or staff.

Where the Trust transfers personal data to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

Subject access requests and other rights of individuals

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 purpose 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
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance of this might be for the individual

Subject access requests might be submitted in writing, either by letter, email or fax to the DPO. Such requests should include:

- The name of the individual requesting subject access
- Correspondence address
- Contact number and email address
- Details of the information requested

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

Children and subject access requests
Personal data about a child belongs to that child, and not to 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.

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 students in the Trust may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to a subject access request
When responding to requests, the Trust:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm that a request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May inform the individual that the Trust will comply with the request within three months, where a request is complex or numerous. The Trust will inform the individual of this within one month and give an explanation of why the extension to the normal access request period is necessary

The Trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if is it repetitive, or asks for further copies of the same information. When the Trust refuses such a request, the individual will be told why, and also informed that they have a right to complain to the ICO.

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 the Trust are collecting their data and how we use and process it (see **Collecting personal data**), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Trust to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge the processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see educational records
Parents, or those with parental responsibility, have a legal right to free access to their child's educational records (which includes most information about a student) within 15 school days of receipt of a written request.

CCTV
The Trust uses CCTV in various locations around school sites to ensure it remains safe. The Trust will adhere to the ICO's code of practice for the use of CCTV.

The Trust is not required to seek individuals' permission to use CCTV, but makes it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any queries about the CCTV system should be directed to the Headteacher).

Photographs and videos
As part of activities within the Trust and its academies/schools, photographs and videos may be taken that record images of individuals.

The Trust will obtain written consent from parents/carers, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where the Trust needs parental consent, it will clearly explain how the photograph and/or video will be used to both the parent/carer

and student. Where the Trust does not require parental consent, it will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within the academy/school on notice boards and in magazines, newsletters, brochures etc.
- Outside of academy/school by external agencies such as photographers used by the Trust, newspapers, campaigns
- Online on the academy/school/Trust website or social media account owned by the Trust

Consent can be refused or withdrawn at any time and if it is withdrawn, the Trust will delete the photograph and video and not distribute it further. When using photographs in this way (or videos) no accompanying information that provides personal data about the child will be used to ensure that they are not identifiable.

Data protection by design and default

The Trust will put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring that they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only process 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 privacy impact assessments where the Trust's processing of 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.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters (a record of attendance at these sessions will be held by the Trust)
- Regularly conducting reviews and audits to test our privacy measures and make sure the Trust is compliant
- Maintaining records of processing activities, including: for the benefit of data subjects, making available the name and contact details of the Trust's DPO and all information the Trust is required to share about how it uses and processes their personal data (via privacy notices); for all personal data that the Trust would hold, maintaining an internal record of the type of data, data subject, how and why the Trust are using that data, any third-party recipients, how and why the Trust are storing data, retention periods and how it is keeping data secure.

Data security and storage of records

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 securely when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, be pinned to notice boards or display boards, or otherwise left elsewhere 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students 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, members, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for trust/academy/school owned equipment (see our acceptable use policy)
- Where the Trust is required to share information with a third party, it must carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

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 cannot or do not need to rectify or update it.

For example, the Trust may shred or incinerate paper-based records, and overwrite or delete electronic files. The Trust may also use a third party to safely dispose of records on the Trust's behalf. If it does so, the third party will be required to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are not personal data breaches. In the unlikely event of a suspected data breach, the Trust will follow the procedure set out under **'**personal data breach procedure'.

When appropriate, the Trust will report the data breach to the ICO within 72 hours. Such breaches in an academy/school context may include, but would not be limited to:

- A non-anonymised dataset being published on the academy/school website which shows the examination results of students eligible for student premium
- Safeguarding information being made available to an unauthorised person
- The theft of an academy academy/school laptop containing non-encrypted personal data about students

Training

All staff, members, 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 processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (Data Protection Act 2018) – if any changes are made to the bill that affect the Trust's practice. Otherwise, or from then on, this policy will see review every 2 years and be shared with the Board.

Links with other policies

This data protection policy is linked with the Trust's other policies:

- Acceptable use policy
- Internet Safety policy
- Mobile data policy
- Cloud security policy

Personal data breach procedure

This procedure is based on guidance on personal data breach produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- 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 or made available to unauthorised people
- The DPO will alert the executive head teacher/head teacher/Head of School and the chair of the Board
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through loss of control of their data, discrimination, identity theft of fraud, financial loss, unauthorised reversal of pseudonymisation (for example, key-coding) – see here, damage to reputation, loss of confidentiality or any other significant economic or social disadvantage to the individuals concerned.

If it is likely that there will be a risk to people's rights or freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's computer systems in a secured folder belonging to the DPO that is sufficiently archived during a backup process. Paper copies are/will be stored in: DPO office
- There the ICO must be notified, the DPO will do this via the report a breach page of the ICO website within 72 hours. As required, the DPO will set out: a description of the nature of personal data breach including where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data items 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 individuals concerned

- If all of the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons for the delay, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out: the name and contact details of the DPO; a description of the likely consequences of the personal data breach and 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 individuals concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. Foe each breach, this record will include the facts and cause, the effects of the breach and any and all action taken to contain the breach and ensure that it does not happen again (such as establishing more robust processes for further training)
- Records of all breaches will be stored on the Trust's computer systems in a secured folder that will be archived regularly
- The DPO and head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will take place as soon as reasonably possible

Actions to minimise the impact of data breaches

The Trust will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly sensitive or risky information. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

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, this can be done through the IT Department as long as the recipient has not opened the email.
- 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 ICT department to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases 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