Data Protection and Information Management Policy

Version 4.0

Important: This document can only be considered valid when viewed on the Trust's website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.	
Name of Author	CEO with support from CFI/Data Protection Officer
Name of Responsible Committee/Individual	Trust Board
Date Policy Agreed	September 2019 (Version 1) December 2020 (Version 2) March 2022 (Version 3) September 2022 (Version 4)
Review Date	March 2023
Target Audience	All Stakeholders
Related Documents	Acceptable Use Policy Freedom of Information Act 2000 Publication Scheme FOI Policy CCTV Policy
References	www.ico.org.uk

CONTENTS

POLICY STATEMENT

The Brighter Futures Learning Partnership Trust understands its obligations under the current Data Protection Act 2018. The Act regulates the use of personal data, and this policy aims to inform anyone in the Trust who comes into contact with data, of their responsibilities; ensuring that they adhere to the Act and minimising the risk of unintentional breaches.

PURPOSE AND SCOPE

The Brighter Futures Learning Partnership Trust has a diverse workforce and individuals in various roles, who come into contact with and use confidential personal information about people (e.g. students, their families, staff and other stakeholders) on a regular basis. The Trust also holds information about every member of staff and staff are required to inform the HR Manager or the School Business Manager of any relevant changes to ensure that the information retained is accurate (e.g. address, contact details, bank details).

This Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

This policy is the Trust's main information governance policy and addresses:

- Data Protection (including rights and complaints)
- Freedom of Information
- Information Asset Management

AIMS AND OBJECTIVES OF THE POLICY

The Brighter Futures Learning Partnership Trust aims to ensure that all personal data collected about staff, students, parents, Trust Members, Trustees, Local Governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (**UK GDPR**) and the ICO's code of practice.

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

LEGISLATION AND GUIDANCE

This policy is to ensure that Brighter Futures Learning Partnership Trust complies with the requirements of the UK General Data Protection Regulation (**UK GDPR**), Data Protection Act 2018 (**The Act**), Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), together with the associated guidance and Codes of Practice issued under the legislation.

DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that The Brighter Futures Learning Partnership Trust 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 Brighter Futures Learning Partnership Trust aims to comply with these principles.

COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

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

- The data needs to be processed so that Brighter Futures Learning Partnership 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 Brighter Futures Learning Partnership Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that The Brighter Futures Learning Partnership 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 Trust 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/student) has freely given clear **consent**
- For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and the Act.

ROLES AND RESPONSIBILITIES

This policy applies to Trust Members, Trustees, Local Governors, **all staff** employed by the Trust, and to external organisations or individuals working on our behalf. Anyone who uses Trust data who do not comply with this policy may face disciplinary action.

The **Trust Board and Local Governing Bodies** will ensure that appropriate policies, procedures, systems and processes are in place within the Trust and each of its schools/the UTC to minimise the risk of a breach of the Act and the UK GDPR.

The **Chief Executive Officer (CEO) and Chief Financial Officer (CFO)** are responsible for the implementation of the policy, ensuring that staff are aware of the expectations surrounding data protection and the potential consequences should a breach occur.

The **Head Teacher/Principal,** as Information Asset owner (IAO) has overall responsibility for ensuring that their Trust school/the UTC complies with all relevant data protection obligations. They are the representative of the data controller for their own school/the UTC on a day-to-day basis. They may delegate this role to a senior leader in the school/the UTC with agreement from the CEO/CFO.

The Trust has appointed Veritau to act as **Data Protection Officer** (DPO). Veritau are part of North Yorkshire Education Services and they are responsible for monitoring compliance with data protection law, and developing related policies and guidelines where applicable. The Trust is responsible for the circulation of appropriate polices, documentation and information to staff in relation to the Act.
The **CEO** is the senior information risk owner (**SIRO**) and the **CFO** is the single point of contact (**SPOC**) for the Trust and is responsible for ensuring all data breaches are logged and reported to the CEO and the Trust Board. Data breaches will also be reported to the DPO and the ICO where deemed necessary.

The CFO will provide an annual report of school/the UTC level activities directly to each school's/Tthe UTC's Local Governing Body. The CFO will also prepare a summary report of all of each school's breaches to the board of trustees, noting their advice and recommendations on any data protection issues. The CFO is also the SPOC for individuals whose data the trust/ school/the UTC processes, and for the ICO.

The Trust's CFO is **Teresa Ladley** and is contactable via the Executive PA on 01302 892937 or email on CFO@brighterfutureslpt.com

The **IT Department or Business Manager** of each school/the UTC is responsible for ensuring that electronic data systems adhere to the requirements of the Act and that there are appropriate mechanisms in place for monitoring and access, such as audit trails, access rights, password and security measures and IT related policies and procedures.

All staff and Officers working on behalf of the Trust are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the trust or their school/the UTC of any changes to their personal data, such as a change of address
- Compliance with the Trust privacy notice for both staff and students
- Contacting the CFO 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
    - With any questions about the operation of this policy
    - 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 European Economic Area
    - 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
- Ensuring contracts / agreements are in place with third parties where personal data is being shared

INFORMATION POLICY

Data Protection

Personal data will be processed in accordance with the requirements of the UK GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (**DPO**). The Trust appointed DPO is Veritau:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01904 554025

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (**ICO**) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

Information Asset Register

The DPO will advise the Trust in developing and maintaining an Information Asset Register (**IAR**). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the Trust will inform the DPO of any significant changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (**IAO**) is the individual responsible for an information asset and understands the value of that information and the potential risks associated with it. The Trust will ensure that IAO's are appointed based on sufficient seniority and level of responsibility. In most cases the IAO is the Headteacher/Principal of the establishment.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when the assets is destroyed, ensuring this is done so securely.

Training

The Trust will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised Trust users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security, including using email and the internet.

The DPO will provide the Trust with adequate training resources and guidance materials. The DPO will be consulted, and will offer an adequacy opinion, if the Trust opts to use a third-party training provider.

The Trust will maintain a 'training schedule' which will record when employees have completed an information governance training module and when a refresher is due to be completed.

The school will ensure that any third-party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

Privacy notices

Brighter Futures Learning Partnership Trust will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on each school's/ the UTC's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents (within their information pack) upon joining one of the Trust schools/THE UTC.

A privacy notice for employees will be provided at commencement of their employment with the Trust. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g., school trips, projects).

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's/the UTC's Information Asset Register.

Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school/the UTC to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any adhoc sharing of information will be done in compliance with our legislative requirements.

Data Protection Impact Assessments (DPIAs)

The school/UTC will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by the UK GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks.

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, and will provide relevant advice.

Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

The Trust has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS).

Destruction of records

Retention periods for records are recorded in the school's/the UTC's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper, to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins.

Advice in regards to the secure destruction of electronic media will be sought from the Trust ICT Manager.

Trust schools and the UTC will retain a Destruction Log (See Appendix A) recording all files destroyed including, where relevant:

- File reference number;
- Description of file;
- Date of disposal;
- Method of disposal; and
- Officer who destroyed record

Third Party Data Processors

All third party contractors who process data on behalf of a school/the UTC must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

Relevant senior leadership may insist that any data processing by a third party ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

Access to information

(1) Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to the Trust CFO by email to: cfo@brighterfutureslpt.com. The CFO is responsible for**:**

- Deciding whether the requested information is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

Freedom of Information Act (**FOIA**) requests should be made in writing. The Trust will only consider requests which provide a valid name and address and will not consider requests which require clicking on electronic links. Environmental Information Regulation (**EIR)** requests can be made verbally, however the Trust will endeavour to follow this up in writing with the requester to ensure accuracy.

Each request received will be acknowledged within 5 school days. The CEO and CFO will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. Advice will be sought from the DPO if deemed necessary. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information;
- Where necessary seek guidance from previous case law in deciding where the balance lies; and
- Consult the DPO

Reasons for disclosing or not disclosing will be recorded on the Trust Central Log of requests and reported to the next Trust board meeting.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.

We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the requester and payment must be received before the information is supplied. Charges will be formulated taking into account the limits set by the legislation.

We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 school days.

(2) Requests for information under the UK GDPR- Subject Access Requests

Requests under this legislation should be made to the Trust CFO by email to: cfo@brighterfutureslpt.com.

Any member of staff may receive a request for an individual's personal information. Whilst the UK GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so and applicants who require assistance should seek help from the school/the UTC. Requests will be logged with the Trust CFO and acknowledged within 5 days.

The Trust must be satisfied as to the requester's identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc); and

- Such further information as may be reasonably necessary to enable the school/the UTC to be satisfied of the applicant's identity.

Only once the Trust is satisfied of the requester's identity and has sufficient information on which to respond to the request will the request be considered valid. The Trust will then respond to the request within the statutory timescale of One Calendar Month.

The Trust can apply a discretionary extension of up a further two calendar months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If the Trust wishes to apply an extension, they will firstly seek guidance from the DPO, before informing the requester of the extension within the first calendar month of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases, the Trust may also refuse a request outright as 'manifestly unreasonable' if it would have to spend an unjustified amount of time and resources to comply.

Should the Trust think any exemptions are applicable, it will seek guidance from the DPO to discuss the request.

For secondary settings only: If a subject access request is made by a parent whose child is 12 years of age or over the Trust may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information) (England) Regulations 2005. Any charges which arise from this request will be applied at the Trust's discretion.

Data Subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the UK GDPR including:

- Right to rectification;
- Right to erasure;
- Right to restrict processing; and
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the Trust CFO by email to cfo@brighterfutureslpt.com who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from the DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Complaints

Complaints in relation to FOI/EIR and Subject Access will be handled through the Trust's existing complaints procedures. Any individual who wishes to make a complaint about the way the Trust have handled their personal data should contact the DPO to the address provided.

Copyright

The Trust will take reasonable steps to inform requesters if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However, it will be the requester's responsibility to ensure that any information provided by the Trust is not re-used in a way which infringes those interests, whether or not any such warning has been given.

DATA BREACH REPORTING

Article 33 of the UK GDPR requires data controllers to report breaches of personal data to the Information Commissioner, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore, it is vital that the Trust has a robust system in place to manage, contain, and report such incidents. The Information Security Incident Management Policy details how the Trust will handle and manage information security incidents when they arise.

Notification and Containment

In order for the Trust to report serious incidents to the ICO within 72 hours it is vital that it has a robust system in place to manage, contain, and report such incidents.

Immediate Actions (Within 24 Hours)

If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the **Specific Point of Contact (SPOC)** within 24 hours. The **SPOC** for the Trust is the Chief Finance Officer (**CFO**). If the **SPOC** is not at work at the time of the notification, then their Out of Office email will nominate another individual to start the investigation process.

If the breach has the potential to have serious or wide-reaching detriment to data subjects, then the Data Protection Officer (**DPO**) **must** be contacted within this 24 hour period.

If appropriate, the individual who discovered the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)

Once received, the **SPOC** will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings can be found in Appendix 1 of this document.

The **SPOC** will notify the **Senior Information Risk Owner (SIRO)** and the relevant **Information Asset Owner (IAO)** that the breach has taken place. The **Senior Information Risk Owner (SIRO)** for the Trust is the Chief Executive officer. The **SPOC** will recommend immediate actions that need to take place to contain the incident.

The **IAO** will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the **Data Protection Officer** (**DPO**) with the assistance of Internal Audit and Counter Fraud Teams.

Reporting to the ICO/Data Subjects (Within 72 Hours)

The **SIRO**, in conjunction with the relevant manager, **SPOC**, **IAO** and **DPO** will make a decision as to whether the incident needs to be reported to the ICO, and also whether any data subjects need to be informed. The **relevant manager/IAO** will be responsible for liaising with data subjects and the **DPO** for liaising with the ICO.

Investigating and Concluding Incidents

The **SPOC** will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

Once the **DPO** has investigated a data breach, the **SIRO** must sign off the investigation report and ensure recommendations are implemented across the Trust.

The **SIRO** will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

All incidences should be recorded on the Central Trust Breach Log, along with the othe UTCome of the investigation.

INFORMATION SECURITY

Access Control

The Trust will maintain control over access to the personal data that it processes. These controls will differ depending on the format of the data and the status of the individual accessing the data. The Trust will maintain an Information Asset Register detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the Information Asset Owner/Administrative staff based at each school/UTC within the Trust.

Manual Filing Systems
Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use. Keys to storage units will be stored securely. The **IAO** will be responsible for giving individuals access to the safe place. Access will only be given to individuals who require it in order to carry out legitimate business functions. Where a PIN is used, the password will be changed every three months or whenever a member of staff leaves the organisation, whichever is sooner.

Electronic Systems
Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. **A two tier authentication system will be implemented across all electronic systems wherever possible. The two tiers will be username and unique password**.

Individuals will be required to change their password every 3 months and usernames will be suspended either when an individual is on long term absence or when an individual leaves employment of the Trust.

Software and Systems Audit Logs
The Trust will ensure wherever possible that all major software and systems have inbuilt audit logs so that the Trust can ensure it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure, it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

Data Shielding
The Trust does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the Trust.

The Trust will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and where possible, any electronic files will be locked down so that the declaring employee cannot access that data.

Employees who knowingly do not declare family and friends registered at the Trust may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

External Access
On occasions, the Trust will need to allow individuals who are not employees of the Trust to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in or because of a Partnership arrangement with another Trust**.** The Chief Executive Officer is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access, then access can also be authorised by the CFO**.**

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the Trust.

Physical Security

The Trust will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by the Trust

Clear Desk Policy
Individuals will not leave personal data unattended on desks or in any other working areas and will use the lockable storage units provided to secure personal data when not in use.

Alarm System
The Trust will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access
External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The Headteacher/principal at each Trust school/THE UTC will be responsible for authorising key distribution on their site and will maintain a log of key holders.

Internal Access
Internal areas that are off limits to pupils and parents will be kept locked and only accessed through PIN or keys. PINs will be changed every six months or whenever a member of staff leaves the organisation. Keys will be kept in a secure location and a log of any keys issued to staff maintained.

Visitor Control
Visitors to the Trust sites will be required to sign in a visitor's book and state their name, organisation, car registration (if applicable) and nature of business. This may be either in paper or electronic format. Visitors will be escorted throughout the building and will not be allowed to access restricted areas without employee supervision.

Visitor books will be locked away at the end of the working day and kept for the current financial year plus six years.

Environmental Security

As well as maintaining high standards of physical security to protect against unauthorised access to personal data, the Trust must also protect data against environmental and natural hazards such as power loss, fire, and floods. It is accepted that these hazards may be beyond the control of Trust, but the Trust will implement the following mitigating controls:

Back Ups
The Trust will back up their electronic data and systems on a daily basis. These backups will be kept off site by an external provider. This arrangement will be governed by a data processing agreement. Should the Trust's electronic systems be compromised by an environmental or natural hazard then the Trust will be able to reinstate the data from the backup with minimal destruction.

Fire Proof Cabinets
The Trust will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records that are held in the cabinets from any minor fires that break out on the building premises.

Fire Doors
Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System
The Trust will maintain a fire alarm system at its premises to alert individuals of potential fires and so that the necessary fire protocols can be followed.

Systems Security

As well as physical security, the Trust also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the Trust's ability to operate and could potentially endanger the lives of its Pupils.

The Trust will implement the following systems security controls in order to mitigate risks to electronic systems:

Software Download Restrictions
Employees must request authorisation from the Trust ICT Manager or member of staff at the site responsible for ICT, before downloading software on to the Trust's IT systems. This person will vet software to confirm its security certificate and to ensure the software is not malicious. The Trust ICT Manager or external provider will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Phishing Emails
In order to avoid the Trust ICT Manager's computer systems from being compromised through phishing emails, employees are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with the Trust ICT Manager or external provider if they are unsure about the validity of an email.

Firewalls and Anti-Virus Software
The Trust will ensure that the firewalls and anti-virus software are installed on electronic devices and routers. The Trust will update the firewalls and anti-virus software when updates are made available and when advised to do so by the Trust ICT Manager or external provider. The Trust will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

Shared Drives
Some schools (including the UTC) within the Trust maintain a shared drive on their servers. Whilst employees are encouraged not to store personal data on the shared drive, it is recognised that on occasion there will be a genuine business requirement to do so. The shared drive will have restricted areas that only authorised employees can access. For example, a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The ICT Manager will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the Trust's retention schedule.

Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the Trust and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The Trust has implemented the following transmission security controls to mitigate these risks:

Sending Personal Data by post
When sending personal data, excluding special category data, by post, the Trust will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending Special Category Data by post
When sending special category data by post the Trust will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive, then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email
The Trust will only send personal data and special category data by email if using a secure email transmission portal such as encrypted, password protected files.

Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s). Use of autocomplete should be strongly discouraged.

Exceptional Circumstances
In exceptional circumstance the Trust may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function
When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then Trust employees will utilise the Blind Copy (BCC) function.

Surveillance Security

Some schools within the Trust operates CCTV at their premises.

Due to the sensitivity of information that could collected as a result of this operation, the Trust has a separate policy which governs the use of CCTV. This policy has been written in accordance with the ICO's Surveillance Code of Practice.

Remote Working

It is understood that on some occasion employees of the Trust will need to work at home or away from the Trust premises. If this is the case, then the employees will adhere to the following controls:

Lockable Storage
If employees are working at home, they will ensure that they have lockable storage to keep personal data and Trust equipment safe from loss or theft.

Employees must not keep personal data or Trust equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or Trust equipment in cars if unsupervised.

Private Working Area
Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use Trust equipment for their own personal use.

Trusted Wi-Fi Connections
Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from the Trust ICT Manager**.**

Encrypted Devices and Email Accounts
Employees will only use Trust issued encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing, or creating personal data. This is because personal devices do not possess the same level of security as a Trust issued device.

Employees will not use Personal email accounts to access or transmit personal data. Employees must only use Trust issued, or Trust authorised, email accounts.

Data Removal and Return
Employees will only take personal data away from the Trust premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to the Trust premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

RECORDS MANAGEMENT

This policy recognises that an effective records management programme is key to facilitating Brighter Futures Learning Partnership Trust's compliance with the legal and regulatory obligations.

Records management is recognised by Brighter Futures Learning Partnership Trust as a core corporate function that supports the effective management of the Trust. A records management programme ensures that authoritative evidence of the Trust's work is created, captured, managed and made accessible within the scope of this policy. This allows for improved accountability, transparency, continuity, decision-making, and better compliance with relevant legislation and regulations, as well as protection of the rights and interests of the school.

A record is defined as '*information created, received and maintained as evidence and as an asset by (the Trust)...in pursuit of legal obligations or in the transaction of business'*.

This policy applies to all records created, received or maintained by staff of the Trust in the course of carrying out its work, whether they are held electronically or in hard copy. Records are retained as evidence for a set period determined by legal, regulatory and functional requirements.

A small proportion of records will be selected for permanent preservation and transferred to an archives service once they are no longer needed by the Trust for current business or legal purposes. This should be done in liaison with the Local Authority Archives Service

Responsibilities

The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Senior Information Risk Owner (**SIRO**) – the Chief Executive Officer of the Trust

The SIRO will act as the accountable person and a champion for records management. They will oversee records management policy and strategy and ensure that the necessary resources are made available and remedial action is taken when problems arise. They will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately and will support appropriate allocation of resources towards the schools'/UTC's records management programme, and will promote records management training for all staff.

The person with operational responsibility for the Trust's records management programme is the Chief Finance Officer. They will ensure that the programme is developed, manage its implementation and overall functioning, including the production of procedures and guidance, work with business units to determine vital records and develop and implement disposal policies and schedules, as well as facilitating programme reviews and improvements.

All staff (including temporary staff) must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the Trust's records management guidelines.

SPECIAL CATEGORY DATA

Brighter Futures Learning Partnership Trust processes special category and criminal conviction data in the course of fulfilling its functions as a multi academy trust. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an '*appropriate policy document'* where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This complements Brighter Futures Learning Partnership Trust's existing records of processing as required by Article 30 of the General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces the Trust's existing retention and security policies, procedures, and other documentation in relation to special category data.

Brighter Futures Learning Partnership Trust is committed to the protection of all special category and criminal convictions data that it processes. This policy applies to all such data whether or not an appropriate policy document is required.

Special categories of data processed

The Trust processes the following special categories of data:

- racial or ethnic origin;
- religious or philosophical beliefs;
- trade union membership;
- health;
- sex life/orientation; and
- Biometric identifier

The Trust also processes criminal convictions data for the purposes identified below.

The Trust relies on the following processing conditions under Article 9 of the General Data Protection Regulation and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Purposes	Examples of use (not exhaustive	Processing conditions
For the provision of education to pupils, including providing support to pupils who are recognised as having Special Educational Needs.	The use of special category data to identify students who require additional support.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To ensure the safety and wellbeing of pupils	Details of safeguarding concerns held in safeguarding files. Allergy and disability information.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
Identification/ authentication	Biometric (fingerprint) school meal payments.	Article 9 (2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
To monitor pupil attendance	Medical reasons for absence.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To maintain records of successful and unsuccessful pupil admissions	Faith school prioritisation of pupils.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of school trips	Provision of dietary requirements to third parties involved with	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and

Purposes	Examples of use (not exhaustive	Processing conditions
	facilitating the school trip.	government purposes
For the provision of education in respect of Looked After Children.	Details of criminal convictions in respect of child's parents.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes.
The management of staff	Personnel files identify medical reasons for absences and trade union membership. Handling of disciplinary proceedings and grievances.	Article 9(2)(b) Employment, social security and social protection Schedule 1 Part 1, 1(a) Processing necessary for the purposes of carrying out obligations and exercising specific rights of the controller and or data subject in the field of employment
Recruitment and pre-employment checks	DBS certificates.	Article 9(2)(b) Employment, social security and social protection Schedule 1 Part 1, 1(a) Processing necessary for the purposes of carrying out obligations and exercising specific rights of the controller and or data subject in the field of employment.
To facilitate the functioning of the governing body	Governors will use special category data where applicable when considering solutions to, for example, access to school for a disabled student.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the prevention and detection of crime	Potential special category and criminal offence data shared	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 5 (10). Preventing or detecting unlawful acts
The handling of complaints	Complaint investigations may involve reference to and use of special category/ criminal conviction data where applicable to the content and nature of the complaint.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To fulfil legislative health and safety requirements	Staff heath information for assessment of reasonable adjustments.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
Equalities monitoring	Collection of staff and student race, ethnicity, and religious background.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes

Compliance with Article 5 – The Data Protection Principles

The Trust maintains documentation and implements procedures which ensures compliance with the Data Protection Principles under Article 5 of the General Data Protection Regulation.

Document/ procedure	Principles	How document procedure aids compliance
Privacy notices	Accountability	The Trust publishes a suite of privacy notices

Document/ procedure	Principles	How document procedure aids compliance
	Lawfulness, fairness, and transparency Purpose limitation Accuracy Storage limitation Data minimisation	which stipulate that the Trust is the 'data controller', the purposes for which the Trust processes special category data and the lawful bases we rely on to do this. This fulfils the Trust's duty to be transparent about the data that it holds, how it is processed and that the Trust as the data controller is accountable. All privacy notices provide details of how to make a data rights request, ensuring that data subjects are able to check and challenge the lawfulness and accuracy of the data processed. Privacy notices are updated where the Trust makes changes to the way it processes personal data.
Policies	Accountability Purpose limitation Storage limitation Security Accuracy Data Minimisation	The Trust maintains a framework of information governance policies (all of which are contained within this Policy document "Data Protection and Information Management Policy" – please refer to the Index on page 2) which detail the expectations and responsibilities of employees of the Trust. This includes, but is not limited to, the following policies: • Information Policy; • Information Security Policy; • Information Security Breach Reporting Policy; • Acceptable Use Policy; • Records Management Policy; • Archive Policy; • CCTV Policy; and • Biometric Data policy These policies set out the processes in place to ensure that the purposes and duration for which special category data are held are not exceeded and the security mechanisms and procedures that are in place to keep this information secure. Administrative procedures for ensuring personal data is recorded accurately and kept up to date are also documented. These policies are reviewed regularly in line with the Trust's policy review schedule to ensure the processes, procedures and measures remain appropriate and effective.
Information Asset Register	Lawfulness, fairness and transparency Purpose limitation Security	Maintenance of this document fulfils the Trust's legal obligation under Article 30 of the General Data Protection Regulation to keep a record of its processing activities.

Document/ procedure	Principles	How document procedure aids compliance
		Information assets which contain special category data have been identified and Article 6, Article 9 and Schedule 1 conditions (where applicable) have been identified for each asset. Retention periods for each asset, based on the Trust's retention schedule, have also been identified, along with the technical and organisational security measures that are in place to protect each asset. This document is reviewed regularly and updated where there have been changes to the Trust's data processing.
Data Protection Impact Assessments (DPIAs)	Accountability Lawfulness fairness and transparency Purpose limitation Data minimisation Accuracy	The Trust conducts Data Protection Impact Assessments where it is undertaking new, high-risk processing, or making significant changes to existing data processing. The purpose of the DPIA is to consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default. All of the data protection principles are assessed to identify specific risks. These risks are then evaluated and solutions to mitigate or eliminate these risks are considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, the Trust will opt to do this. All DPIAs are signed by the Trust's Senior Information Risk Owner and Data Protection Officer.
Mandatory data protection training	Accountability Security	All staff undertake mandatory data protection training, which is refreshed every 2 years with annual refresher/reminder training Staff members who have particular responsibility for managing the risks to personal data, such as the Senior Information Risk Owner, Specific Point of Contact and Information Asset Owners, undertake additional specialist training where applicable. Where new processes are introduced as a result of additions to or changes to processing, additional training will be provided to staff members involved with the project. The requirement for this will be identified as part of Data Protection Impact Assessments.
Retention schedule and destruction log	Purpose limitation Data minimisation	The Trust does not retain special categories of data for any longer than it is necessary to do so in order to fulfil our specific purposes.

Document/ procedure	Principles	How document procedure aids compliance
		The Trust has a retention schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). Where there is no legislative or best practice guidance in place, the Senior Information Risk Owner will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. The information asset Owner has responsibility for ensuring records retention periods are adhered to. The Trust also maintains a destruction log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed.
Technical and organisational security measures and procedures. Recording and reporting personal data breaches where necessary	Security Accountability Accuracy	The Trust employs the following technical and organisational security measures where appropriate to protect the personal and special category data that the Trust processes • Password protection of electronic devices and systems • Encryption of portable devices • Encryption of emails • Recorded delivery of sensitive paper documents • Secure, fireproof storage of paper records using a key/ PIN management system • Clear desk policy • Audit trails on electronic systems where possible • Regular backups that can be restored in the event of an emergency • Access/ permission controls • Secure destruction of paper records • Information governance policies (detailed above) • Physical building security measures (locked doors, visitor sign in procedure alarm system, CCTV etc.) • Cyber security risk prevention measures (firewalls and anti-virus software, phishing email awareness, download restrictions etc.) A full description of security measures employed by the Trust can be found in the Trust Information Security Policy referenced above. In the event that these measures should fail, and a personal data breach occurs, the incident will be recorded in a log, investigated and reported to the Trust Data Protection Officer

Document/ procedure	Principles	How document procedure aids compliance
		where necessary. Severe incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in the Information Security Breach Reporting Policy referred to above.
Written contracts with data processors	Accountability Security	Where the Trust shares personal data with a data processor, a written contract is obtained. All existing contracts are checked to ensure that all mandatory data protection clauses are present, and all new contracts are assessed prior to forming an agreement with the processor.
Compliance with data rights requests	Lawfulness, fairness and transparency Accountability Accuracy	The Trust maintains a log of all data rights requests and has appropriate processes set out in the Trust policies for handling such requests.
Data Protection Officer	Accountability	The Trust has appointed a Data Protection Officer to oversee the Trust's compliance with the data protection principles.

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in the Trust retention schedule, which is based on the Information and Records Management Society (IRMS) Toolkit for Schools. Retention periods of specific information assets are identified in the Trust's information asset register and the Trust has adopted a Records Management Policy, as referred to above.

ACCEPTABLE USE

This section governs the use of the Trust's corporate network that individuals use on a daily basis in order to carry out business functions.

Email

The Trust provides email accounts to employees to assist with performance of their duties.

Personal Use
Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of the Trust,
- Employees understand that emails sent to and from corporate accounts are the property of the Trust,
- Employees understand that Trust and school management may have access to their email account and any personal messages contained within,
- Employees understand that the Emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the Trust reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network; and
- Use of corporate email accounts for personal use does not infringe on business functions.

Inappropriate Use

The Trust does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files,
- Unwelcome propositions,
- Profanity, obscenity, slander, or libel,
- Ethnic, religious, or racial slurs,
- Political beliefs or commentary and
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Other Business Use
Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises.

Email Security
Users will take care to use their email accounts in accordance with the Trust's information security policy. In particular, users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the Trust's IT network; or
- Not send excessively large email attachments without authorisation from the Trust ICT Manager.

Group Email Accounts
Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. The Chief Executive Officer in consultation with the Trust ICT Manager will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

The Trust may monitor and review all email traffic that comes to and from individual and group email accounts.

Internet Use
The Trust provides internet access to employees to assist with performance of their duties.

Personal Use
Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the Trust,
- Employees understand that Trust management may have access to their internet browsers and browsing history contained within,
- Employees understand that the Trust reserves the right to suspend internet access at any time; and
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

The Trust does not permit individuals to use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs; and
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises.

Internet Security

Users will take care to use the internet in accordance with the Trust's Information Security Policy. In particular users will not click on links on un-trusted or unverified WebPages.

Social Media Use

The Trust recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The Trust also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time. In addition to the below the Trust **Social Media Policy** should be read in conjunction with this policy.

Corporate Accounts

Some schools (including the UTC) in the Trust have social media accounts across multiple platforms. Nominated employees will have access to these accounts and are permitted to post general information about the Trust and its schools. Authorised employees will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. The CEO, in consultation with Headteachers/Principal and the Trust ICT Manager, will have overall responsibility for allowing access to social media accounts.

Corporate Social Media Accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the Trust's information governance policies and data protection legislation.

Corporate Social Media Accounts must not be used in a way which could:

- Tarnish the reputation of the Trust,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Be construed as sexually explicit; or
- Be construed as political beliefs or commentary.

Personal Accounts

The Trust understands that many employees will use or have access to Personal Social Media Accounts. Employees must not use these accounts:

- During working hours,

- Using corporate equipment,
- To conduct corporate business; or
- To contact or approach clients, customers, or partners of the schools/UTC.

Telephone Use
The Trust telephony network is provided to employees to assist with performance of their duties. This may include Skype for Business and for the benefit of doubt Skype calls are classed as telephone calls in this policy.

Personal Use
Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:
- Usage does not tarnish the reputation of the Trust,
- Employees understand that Trust management may have access to call history,
- Employees understand that the Trust reserves the right to suspend telephone usage at any time,
- Use of the telephone for personal use does not infringe on business functions; and
- Employees understand that there may be a charge for personal usage.

Inappropriate Use
The Trust does not permit individuals to use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use
Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises.

Telephone Conduct
In general terms users should conduct themselves in a professional manner when using the telephone and always adhere to the requirements of the Trust Code of Conduct.

ACCESSING CLOUD SERVICE ON PERSONAL DEVICES

This section governs the use of personal devices to access the personal data held in Cloud based systems and processed by the Trust. It applies to all personal data and any operational data that is classified as 'sensitive or confidential' that is held in in one of the Trust's systems and accessed through a non-school provided device.

During the pandemic remote working was developed across all organisations and software developers have taken steps to ensure access to data is readily available and without the constraints of being held within a restricted network. There has been a move by many organisations to transfer their locally held data into the 'Cloud', enabling access by any internet connected device, anywhere in the world.

Being able to access data promptly; the financial savings for not having to provide devices to all relevant personnel; and individuals being able to use devices of their choice are all benefits that Cloud computing has brought to education.

With this enhanced access and benefits comes a high level of risk that the Trust needs to consider and mitigate through the use of technical controls, expected behaviours and supporting policies. This policy aims to provide the framework for adequate management of the risks posed.

The Trust identifies a personal device as any electronic device that can be used to access and process personal data, including data accessed from the Cloud through an internet connection. This includes, but it not limited to:

- Laptop/PC;
- Notebook;
- iPad; and
- Smart Phone

Use of the device must be limited to the individual, and not be shared resources (e.g. a family device).

Device Security

Anti-virus and software security patching
The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the individual to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

The Trust requires that any device used for accessing school systems in the Cloud must have adequate anti-virus software where available. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that are going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access Trust data.

Password/PIN protection
All devices must be secured by a unique password or security pin to ensure that access to the device is limited to named individual permitted to access the Trust personal data. Devices that lack the ability to enforce this level of security must not be used for access Trust data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. A robust password would provide an additional layer of protection.

Personal apps
Individuals are asked to be mindful of the apps installed on personal devices that they use to access Trust data. Some of these apps may have enhanced privileges and tracking within them that monitors use of the device and other items that are being accessed. This should be detailed in the apps terms and conditions and the individual should seek assurance that this risk is being managed.

Equipment disposal
When a device being used to access school information is disposed of, it is the responsibility of the individual, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

Physical security
Individuals should ensure any device used to access Trust data is kept safely and secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, transported without sufficient protection to prevent accidental damage etc.

Email and Internet Activity

Inappropriate use

The Trust does not permit individuals to use Trust email accounts to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Access to websites that contain similar content is also not permitted when obtained via Trust systems. Full details of what is deemed inappropriate can be found in the Acceptable Use Policy.

Use of personal email accounts
The Trust does not permit any individual to use personal email accounts when processing personal data from the Trust, and therefore information cannot be sent to private email accounts for accessing outside of the Trust systems.

System and Accounts Security

When accessing data held in the Cloud via an internet connection (e.g. Microsoft 365), individuals must ensure that their account is closed when not in use by logging out of the system. It is not permitted for access to accounts on any of the Trust systems to be open when not in use.

Individuals are responsible for ensuring any internet connection used to access Trust data must be secured through the use of access controls (a specific user name and password). Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices must be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

Permitted Activity

Whilst using their own devices, individuals are permitted to access, review and process personal data within the Trust system with which it is held (e.g. Outlook when responding to an email).

It is not permitted for the data to be downloaded and saved onto any personal device under any circumstances. All Trust data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within the Trust records management system for its full life cycle, including secure destruction in line with the Trusts retention schedule.

By retaining data within Trust controlled systems, in the event of an individual exercising their rights as detailed in the UK General Data Protection Regulation (**UK GDPR**); particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require individuals to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

Data Breaches

In the event of a data breach individuals must follow the process detailed in this Policy. The risk of a data breach increases in the following situations:

- Access to systems is not closed appropriately when not in use
- Personal devices are shared with family/friends/partners
- Documents and files are downloaded onto share devices, and then become accessible to other users of the device.
- Passwords/security PINs are shared with others (e.g. family and partners); leading to the potential of unauthorised access to devices
- Inadequate management of security and software updates leaves a vulnerability to a virus/hack. Once unauthorised control of a device is established it is difficult to identify and remove and
- Disposal of devices that have not been adequately assessed and the permanent removal of any school related data prior to surrender.

Individuals are therefore encouraged to be mindful in all these situations.

Exemption Process

An exemption to any element of this policy can only be authorised by the CEO who is the Trust's Senior Information Risk Owner (**SIRO**). Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated. For example, adequate mitigation measures to protect any personal data processed could include a strict requirement for the relevant staff member to delete the data from their device after use and confirm in writing to the SIRO once complete.

Authorised Access

Access to Trust systems using personal devices is only permitted whilst an individual has authorisation to do so. In the event that the individual leaves the employment of the Trust; or the relationship terminates for third parties and contractors; access should not be attempted. To do so would be treated as an information security incident (data breach) and investigated as such.

It is a criminal offence under Section 170 of the Data Protection Act 2018 (**DPA**)to knowingly access data that you are not entitled to or after you have left the employment of that employer.

ARCHIVE POLICY

This section outlines how the Trust will maintain a record of its former pupils and staff in such a way as to comply with the UK GDPR and DPA. It is based on compliance with Article 5 (the principles) and on Article 89 (safeguards and derogations).

Brighter Futures Learning Partnership Trust wishes to create and preserve an organisational memory of its history, including its pupils and staff. This organisational memory is expected to contribute to the wider social memory of the community which the school serves.

In general, records of pupils and staff are to be destroyed once their purpose is complete. However, the Trust wishes to maintain a record of its own history, and its role within the community, rather than simply forgetting those individuals completely, which is what would happen if the retention schedule is applied in full.

This policy sets out exceptions to that schedule. In order to remain compliant there are some criteria to apply which are set out below, covering the selection of data, and limits on how personal data found in the archive can be used.

Use of archive records

Uses for the archive might include:

- Historical displays by the Trust or community, perhaps when a significant anniversary occurs
- Loan of items to museums or other archives for their own displays or exhibitions
- Academic research into educational, social or other topics; and
- Reference to individuals if they become a focus of interest in the future (although subject to their reasonable expectations of privacy)

Any use of the archive will be constrained as follows:

- No decision may be made about an individual using his or her data drawn from the archive
- No unwarranted harm or distress should be caused to an individual by the inclusion or use of his or her data in the archive; and
- Where a purpose can be fulfilled using anonymous or pseudonymous data, then only anonymised or pseudonymised data will be disclosed

Anonymisation before further use or processing is the default, although it is likely very many uses (especially exhibitions and displays) will require fully identifiable data

Security and control of the archive

The archive will become another information asset and as such should be added to the information asset register.

The Trust considers that its archive does fulfil a public interest in maintaining its own memory and that of the community. The UK GDPR provides that an archive maintained in the public interest is not incompatible with the original purpose for which the data was collected.

The information asset owner will be the trust Chief Finance Officer who is also the SPOC (Single Point of Contact) for the Trust. This person will ensure that the archive is subject to security measures, including:

- authorising disclosure to those wishing to use or access it (or refusing it)
- ensuring it is protected from loss or corruption (including as appropriate a catalogue; a recording out and in system; allowing only copies to be loaned or displayed)
- applying suitable contractual or other controls to ensure the constraints set out above are observed; and
- anonymising material before disclosure, unless the intended use requires identifiable data.

The asset owner will also ensure that new data sets are added to the archive at each year end or at other appropriate times.

Data subjects' rights

In general data subjects have the same rights over their data in the archive as anywhere else. The information asset owner will decide how to respond to requests to exert those rights.

Right be informed: reference to this policy will be included in relevant privacy notices.

Subject access: there is no need to search for or disclose data held only in the archive in response to a subject access request if to do so would require disproportionate effort.

Erasure: as the archive is maintained in the public interest erasure will usually be refused unless a compelling case for it is made. Note that although data subjects may have been children when their data was collected this was not for the purpose of online ("information society") services, nor in reliance on their consent.

References

The UK GDPR Article 5(1)(e): non-retention of personally identifiable data

Article 89 (Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) and recitals 26, 29, 33, 50, 60, 61, 62, 75, 78, 156,

DPA 2018, Section 19 of which provides further safeguards and restrictions. In particular, this means those wishing to use personal data from the archive must:

- be able to demonstrate why they cannot use anonymised data;
- consider whether they could use pseudonymisation to make it more difficult to link the personal data back to specific individuals;
- be able to demonstrate that the processing is not likely to cause substantial damage or distress to individuals;

- not use the data to take any action or make decisions in relation to the individuals concerned (unless carrying out approved medical research as defined in section 19(4) of the DPA 2018); and
- consider other appropriate safeguards and security measures.

BIOMETRIC DATA

This section fulfils the Brighter Futures Learning Partnership Trust's obligation to have an appropriate policy document in place where the processing of Special Category Biometric data is in place.

It governs the Trust's collection and processing of biometric data. The nature of this processing, including what information is processed and for what purpose, is outlined in the Trust's privacy notices.

The Trust will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012, this includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to the requirements of the UK General Data Protection Regulation (**UK GDPR**).

This policy complements the Trust's existing records of processing required under Article 30 of the UK GDPR, which is fulfilled through the Information Asset Registers held within each of the Trust schools/the UTC. It should also be read in conjunction with the other policies and privacy notices in the Trust's Information Governance policy and privacy notice framework.

Definition of "Biometric Data"

Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual. For example, where a fingerprint is used to identify an individual and allow them access to an account.

Biometric Data is defined in the UK GDPR and the Data Protection Act 2018 (**DPA**) as a special category of personal data, and it therefore requires additional measures to be put in place in order to process it, as detailed below.

Definition of "Processing"

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) Storing pupils' biometric information on a database system; or

c) Using that data as part of an electronic process**,** for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

Any processing of Biometric data will only be carried out where there is a lawful purpose for the processing, as defined under Article 6 and Article 9 (Schedule 1) of the UK GDPR. The purposes will be outlined in the Trust's privacy notices which will be made available to the relevant individuals.

What Counts as Valid Consent?

The DPA states that an individual can consent to the use of their own personal data when they are considered to have the adequate capacity to fully understand what they are consenting to. Most individuals are considered to reach this capacity over the age of 12, however where the Trust considers the individual to not have adequate capacity to consent themselves, the consent of one or more of their parents/carers will be sought.

The Trust will ensure that the member of staff, or the student and both of their parents/carers (if possible) will be informed of the Trust's intention to process the individual's biometric data. This will be carried out through readily available privacy notices and communications, prior to or at the point of obtaining consent, and will include:

- The type of biometric data
- What it will be used for
- The parent's and pupil's rights to withdraw or refuse consent; and
- What the alternative arrangement will be if consent is refused or withdrawn

Under no circumstances will the Trust collect or process the biometric data of an individual without their explicit consent or the consent of at least one authorised parent/carer, this will be obtained prior to obtaining any biometric data. If one parent objects in writing, then the Trust will not be permitted to take or use that child's biometric data.

All consent must be freely given, specific, informed and unambiguous, and will be obtained through a clear affirmative action. The Trust will collect consent by including Biometric data, and its use, on the Parental Consent Form for new starters.

Where the Trust collects additional Biometric data or begins to process the biometric data for a new purpose, new consent must be gained to ensure that the individual or their parent/carer is fully informed. This consent must also meet all of the standards outlined in this section.

The Protection of Freedoms Act 2012 only covers processing on behalf of the Trust. If a pupil is using biometric software for their own personal purposes (e.g. facial recognition technology) this is classed as private use not processing by the Trust, even if the software is accessed using school or college equipment.

Length of Consent and Withdrawing Consent

The consent will be valid until it is withdrawn or until the Biometric data reaches the Trust's retention period, when the student leaves the Trust, at which point the Biometric data will be securely destroyed.

Consent can be withdrawn at any time by the parent/carer or the individual, by contacting the Trust school/the UTC directly. Contact details of the appropriate person are contained on the Parental Consent Form.

If a student under the age of 18 objects to the processing of their Biometric data, this will override the consent of the parents/carers and processing will not continue under any circumstances.

Alternative to Biometric Data

The Trust will ensure that where consent is refused or withdrawn there is an alternative solution which does not require the obtaining or processing of Biometric data. This will ensure that the consent is freely given and that no pressure is placed on the individual or their parent/carer to consent in order to take part in the Trust processes.

Data Protection Impact Assessment

Where a new system involving Biometric data, or a new form of processing for Biometric data is introduced, the Trust will ensure that they have completed a Data Protection Impact Assessment (**DPIA**) to address any risks associated with the project prior to the implementation of the project. This will be sent to the School's Data Protection Officer for final approval.

CCTV

This section concerns the use and governance with regards to the systems; and the processing of personal data which has been collected by using surveillance technology. The policy is written in accordance with various data protection legislation, and the Information Commissioner's Office's (ICO) Surveillance Code of Practice.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The Trust only uses surveillance in the context of CCTV.

The Trust does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

The Trust operates 'Closed Circuit Television' (CCTV) systems:

- for the prevention, reduction, detection and investigation of crime and other incidents;
- to ensure the safety of staff, students and visitors;
- to assist in the investigation of suspected breaches of Trust regulations by staff or students; and
- the monitoring and enforcement of traffic related matters (where applicable).

Planning CCTV Systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The Trust has various statutory responsibilities to protect the privacy rights of data subjects. Therefore during this planning phase, the Trust will consider:

i. The purpose of the system and any risks to the privacy of data subjects,

ii. That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).

iii. The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system must record with sufficient resolution to perform its task.

iv. The system must also have a set retention period (the typical retention period is one month) and, where appropriate, the Trust must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects and

v. That the Trust will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The Trust will ensure that a contract will be agreed between the Trust (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the Trust.

CCTV Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore, the use of CCTV systems must be visibly signed.

The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data. The Trust CCTV Privacy notice is available on the Trust website

Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining a CCTV system is to prevent and detect crime then the footage must only be examined where there is evidence to suggest criminal activity having taken place.

The CCTV system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the School's Information Policy.

If the school receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

i. the purpose of the request,
ii. that agency's lawful basis for processing the footage,
iii. confirmation that not receiving the information will prejudice their investigation; and
iv. whether the school/the UTC can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The school/the UTC will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

Review of CCTV

CCTV systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The Information Asset Owner should use the checklist included in

Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asser Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

Complaints

Complaints by individuals about the use of CCTV systems, or the way CCTV data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware.

DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data; and • 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.
Special categories of 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; and • Sex life or sexual orientation

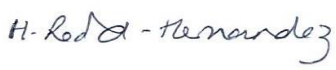
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Third Party 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

MONITORING ARRANGEMENTS

The CFO is responsible for monitoring and reviewing this policy, which will be reviewed every 2 years.

Data Protection Policy Agreed: September 2022

Signed CEO of BFLPT – Helen-Redford-Hernandez:



Date: September 2022

Signed – Chair of BFLPT – Marcus Isman-Egal:

Date: September 2022

Data Protection Policy to be reviewed: March 2023
Created: September 2019 (Version 1)
Revised: December 2020 (Version 2)
March 2022 (Version 3)
September 2022 (Version 4)

XX School Name XX - Data Destruction Log

Staff member responsible for the maintenance of this destruction log: (Job title. Please ensure that the staff member is appropriately placed, and is aware of their responsibility.)

Name of Information Asset	Asset Owner's Job Title	Description of information (what was purpose etc)	Format (electronic / paper etc)	Date Information Created (or range of dates)	Retention Period	Date Destroyed	Method of Destruction	Name (and job title) of staff member who deleted data	Authorised by Information Asset Owner?	Comments/Notes
eg. List of pupils on Free School meals	*Headteacher/SIRO etc*	*eg. correspondence about, list of pupils, pupil info, dietry requirements for the purpose*	*Electronic*	*Sept 1995 - 1996*	*10 years*	*10-Sep-05*	*Deleted from School systems*		*Y*	