Bright Futures

EDUCATIONAL TRUST

The best *for* everyone, the best *from* everyone

Combined Data Privacy Policy
-Staff
-pupils, parents/carers

This is a Trust-Wide Policy

which applies to all the schools within the Trust

Date of Policy Approval:	18 June 2018
Owner of Policy:	Data Protection Officer
Authorised By:	Board of Trustees
Policy Review Date:	June 2019
Distribution:	**All staff, workers, governors and trustees** **Staff Shared drives only**

CONTENTS

DATA PRIVACY POLICY
COMBINED POLICY FOR THE ATTENTION OF ALL STAFF
STAFF, PUPILS, PARENTS/CARERS DATA PRIVACY

Bright Futures Educational Trust's (BFET or the Trust) Strategy underpins all aspects of this policy and the way in which it will be applied. These elements are:

- Our vision, the best ***for*** everyone and the best ***from*** everyone;
- Two of our values; **Integrity**: We do the right things for the right reasons and **Passion**: We take responsibility, work hard and have high aspirations;
- Two of our commitments: **Effective Communication** and **Strong Governance and Accountability.**

PART ONE –STAFF DATA PRIVACY POLICY

What is the Policy for?

This policy contains important information about how and why Bright Futures Educational Trust ("the **Trust**") collects, processes, stores and shares personal data belonging to our employees, workers and third parties e.g. pupils and parents (**Third Party Data**).
The focus of this policy is on the Trust's duties and responsibilities in respect of the personal data of our employees and workers (**Staff**), and the duties and responsibilities our Staff have to Process the personal data of our Staff and Third Party Data in accordance with our policies, procedures and the law.
This Data Privacy Policy should be read in conjunction with our:

- Data Privacy Policy –Education, for pupils and parents;
- Privacy Notice for Staff;
- Disciplinary Policy and Procedure.
- E-Safety Policy

By Trust we mean, all academies in the Trust and the head office of the Trust

Who is the Policy for?

Part One of this policy is for the attention of anyone who is employed by, provides a service to, or volunteers to work at the Trust and its academies. This includes governors and trustees.

Part Two of this policy is for pupils and parents/cares to understand how their personal data will be handled. It is also for staff to understand their responsibilities in handling the personal data of pupils, parents and carers. It is published on our website.

About this policy

In legal terms, this process of collecting and processing personal data means that the Trust is referred to as a Controller (**Controller**). Any external person or organisation that processes personal data on our behalf and on our instructions (e.g. a payroll provider or insurance company) is referred to a Data Processor (**Processor**).
Any activity that involves the use of personal data is referred to as Processing (**Processing/Process/Processes**). It includes:

- Obtaining, recording or holding personal data;
- Carrying out any operation or set of operations on personal data (e.g. organising, amending, retrieving, using, disclosing, erasing or destroying it); and
- Transmitting or transferring personal data to third parties.

Personal data is any information identifying or relating to an identifiable data subject (**personal data**). A person is considered to be a Data Subject if he or she is a living individual that can be identified (directly or indirectly) from the personal data (**Data Subject**). Personal data includes some Special Category Data and Criminal Conviction Data. The following table gives a non-exhaustive list of examples of what is included and excluded from these definitions:

Personal data		
Personal data	**Special Category & Criminal Conviction Data (formerly called Sensitive Personal data)**	**Excluded / Not Personal data**
• Name • Address • Telephone number • Date of birth • Gender • Qualifications • Opinions about an individual's actions or behaviour (e.g. references, Staff appraisals, disciplinary records) • Location data • Images e.g. CCTV, photographs	• Racial or ethnic origin • Political opinions • Religious or similar beliefs • Trade union membership • Physical or mental health conditions (e.g. sick notes, medical reports) • Sexual life • Sexual orientation • Biometric or genetic data • Criminal offences and convictions (e.g. DBS checks)	• Anonymous data • Data that has had the individual's identity permanently removed (e.g. statistical information about the gender breakdown of our Staff from whom individuals cannot be identified)

Policy Standards

1. Your rights as a Data Subject

Each Data Subject has legal rights designed to protect the privacy of their personal data. You are a Data Subject (with regard to your own personal data). This Staff Data Privacy Policy explains more about your rights as a Data Subject and your responsibilities in relation to processing personal data of third parties.

2. Third Party Data: your duties and responsibilities

To the extent that you are involved in the processing of personal data, you will have legal duties and responsibilities to process the personal data of others in accordance with this Data Privacy Policy, the Data Privacy Policy-Education, which applies to the personal data of our pupils, parents/carers etc, and the law governing data privacy, including the GDPR and Data Protection Act 2018 (see "Our commitment to complying with data protection procedures" below).
If your role involves regular processing of personal data, or might reasonably bring you into contact with Personal data, you will receive training on our data privacy policies and procedures as

part of your induction and this will be refreshed at regular intervals thereafter (see "Staff Training" below).

3. Data privacy: our collective responsibility

The Trust takes its legal obligations and responsibilities regarding data privacy very seriously. We expect all of our staff to treat any personal data they may come into contact with (whether it is part of their role to handle such data or not) sensitively and in accordance with our data privacy policies and procedures. You are reminded that any breach of this policy, our data privacy procedures, or the law governing data privacy, may result in disciplinary action.

4. Our Commitment to complying with the Data Protection Principles

Personal data must be processed in compliance with the Data Protection Principles (**DPP**) relating to the Processing of personal data (as set out in the General Data Protection Regulation (EU 2016/679) (**GDPR**). The DPP require personal data to be:

Data Protection Principle (DPP)	**Details**
Processed lawfully, fairly and in a transparent manner	Personal data must be processed on the basis of one or more of the conditions specified in the GDPR.
Collected only for specified, explicit and legitimate purposes.	If we collect personal data directly from Data Subjects, we will inform the Data Subject about: • The Purpose(s) for which we intend to Process their personal data; • The third parties (if any) with which we will share, or to which we will disclose, their personal data; and • Their rights as a Data Subject (e.g. to access and rectify their personal data). Personal data must not be processed in any manner incompatible with those original purposes.
Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.	We will only collect personal data to the extent that it is required for the specific Purpose notified to the Data Subject.
Accurate and where necessary kept up to date	We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You are required to keep us informed of any changes to your personal data so that we can keep our records accurate We will take all reasonable steps to, without delay, destroy or amend inaccurate or out-of-date personal data.

Not kept in a form which permits identification of a Data Subject for longer than is necessary for the purposes for which the data is processed.	We follow current data retention guidelines and have procedures for the deletion and destruction of data in accordance with those guidelines.
Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.	We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We have put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they also put in place adequate security measures.
Made available to the data subject on request and that Data Subjects are allowed to exercise certain rights in relation to their personal data	We will process all personal data in line with data subjects' rights, in particular their right to: • Request access to any personal data held about them; • Prevent the processing of their personal data for direct-marketing purposes; • Ask to have inaccurate personal data amended; and • Prevent Processing that is likely to cause damage or distress to themselves or anyone else.
Not transferred to people/organisations situated in countries without adequate protection	We may only transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies: • The country ensures an adequate level of protection for the Data Subjects' rights and freedoms; • The data subject has given consent; • The transfer is necessary for one of the conditions set out in the GDPR (e.g. for the performance of a contract between us and the data subject, or to protect the vital interests of the data subject); • The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

	• The transfer is authorised by the Information Commissioner where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

5. Conditions for processing

To be processed lawfully, personal data must be processed on the basis of one or more of the conditions specified in the GDPR (**Condition(s)**). The most common conditions we rely on to process personal data are:

Conditions for processing staff personal data which we commonly rely on	
Personal data	**Special Category Personal data & Criminal Convictions Data (formerly called Sensitive Personal data)**
• The data subject has given his consent to the processing for one or more specific purposes; • Processing is necessary for entering or performing a contract with the data subject; • Processing is necessary for compliance with a legal obligation to which the Controller is subject; • Processing is necessary to protect the vital interests of the data subject; or • Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party.	• The data subject has given explicit consent to the processing for one or more specific purposes; • Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection lawso far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; • Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent; • Processing is necessary for the establishment, exercise or defence of legal claims; or • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

However, we may in some circumstances rely on other conditions set out in the GDPR or Data Protection Act 2018 to justify the processing of personal data, special category personal data or criminal conviction data.
Personal data must only be collected or processed for specified, explicit and legitimate purposes. The Trust will establish and record the condition for processing each time processing of personal data occurs.
Staff are forbidden from processing personal data for purposes which go beyond or are incompatible with the original purposes specified to the data subject in the transparency information provided to them (see "Transparency: notifying Data Subjects" below).

6. Consent

Consent is one of the many conditions upon which the processing of personal data can be based. However, in lots of circumstances the Trust will rely on other conditions to process personal data. For example, the Trust do not routinely rely on consent as a condition to justify the processing the personal data of our staff. This is explained further in your personal Privacy Notice for School Staff.
Key points to note about relying on consent as a Condition for Processing:

- Consent requires affirmative action; silence, pre-ticked boxes or inactivity should not be considered to be consent;
- Consent must be kept separate from other terms and conditions, so that it is clear and unambiguous;
- Use clear and plain language when explaining consent;
- Consent must be specific and informed, meaning it should be clear to the Data Subject what it is they are consenting to and how and why their Personal data will be processed;
- The data subject must be free to refuse to give their consent to the processing;
- If consent is relied upon, the data subject must be easily able to withdraw their consent to processing at any time and withdrawal must be promptly honoured;
- Consent should be refreshed if personal data will be processed for a different and incompatible purpose to that disclosed when the data subject first consented;
- Consent should not be relied upon as a condition for processing where there is an imbalance of power between the Trust and the data subject; and
- Records should be kept of any consent received (what consent was given, when and how it was obtained).

7. Rights of Data Subjects

Data Subjects have rights when it comes to how we handle their personal data. Some of these rights are dependent on the nature and purposes of the processing. In summary, these include rights to:

- Withdraw consent to processing at any time where we have relied on consent to conduct the processing (see above "Consent");
- Receive certain information about our processing activities (see "Transparency: notifying Data Subjects" below);
- Request access to the personal data that we hold on them (see "Subject Access Requests" below);
- Prevent our use of their personal data for direct marketing purposes;

- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed, or to rectify inaccurate data or to complete incomplete data;
- Restrict processing in specific circumstances;
- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- Request a copy of an agreement under which personal data is transferred outside of the EEA;
- Prevent processing that is likely to cause damage or distress to them or anyone else;
- Be notified of any personal data breach which is likely to result in a high risk to their rights and freedoms;
- Make a complaint to the Information Commissioner; and
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Staff who wish to exercise a right on their own behalf or who receive a written request from a data subject who wishes to exercise any of their GDPR or data privacy rights (for example, requesting the rectification or deletion of their Personal data) should contact our Data Protection Officer: dataprotection@bfet.uk, immediately.

Subject Access Requests

Data Subjects may make a formal written request for details of the personal data we hold about them (**Subject Access Request**). The GDPR requires us to deal with Subject Access Requests within strict time-limits. Once the identity of the requestor is verified, the information will be provided within 30 calendar days. If the request is complex, numerous or arrives during the school holidays and records cannot be accessed the Trust has the right to determine that up to a further 2 months is required to respond to a subject access request. The DPO will write to the data subject within a month of their written request to set out the reasons why the time is being extended.
Therefore, staff who receive a written or oral request for access to personal data (whether or not the request specifies that it is a Subject Access Request) should forward it to our Data Protection Officer immediately. However, if the request is limited to a specific document or piece of information and could more simply be dealt with by the member of staff who received the request through their day-to-day role, it is permissible to deal with the matter on an informal basis. Should you have any queries, please consult our Data Protection Officer.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if we check the caller's identity to make sure that information is only given to a person who is entitled to it. If we are not sure about the caller's identity, or if their identity cannot be checked, we will ask that the caller put their request in writing.

8. Transparency: Notifying Data Subjects

The GDPR requires controllers to provide clear, detailed and specific information to data subjects about the processing of the Personal data. Such information must be provided through appropriate privacy notices. Our Privacy Notice for School Staff sets out the information about how we process your Personal data. It will be reviewed annually to ensure we are as transparent as possible about the Personal data we process.

The GDPR (and the accompanying guidance) is very specific about the language used in any privacy notices. To ensure compliance with the GDPR the Data Protection Officer must be involved in the drafting of any privacy notices.

9. Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes (**purposes**) and must not be further processed in any manner incompatible with those Purposes. This means that we cannot use Personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new Purposes, and (if this is the Condition relied upon to Process their Personal data) they have given their Consent. To ensure compliance with this Purpose limitation requirement:
The Trust will establish and record the purposes for processing personal data on its record of processing activities;

- Staff who are responsible processing personal data must ensure on each occasion that the Purposes for doing so are not incompatible than the original specified purposes. If the purposes are incompatible, the Data Subject must be notified of the new Purposes as soon as possible.

You are reminded that processing personal data for purposes which are incompatible with the purposes for which the personal data was obtained is considered a serious breach of this Data Privacy Policy and may result in disciplinary action.

10. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that you:
May only collect or Process Personal data when performing your job duties requires it;

- Cannot Process personal data for any reason unrelated to your job duties;
- Must not collect excessive personal data, which is not relevant for the specified purposes;
- Must ensure that when any personal data is no longer needed for the specified purposes, it is deleted or anonymised in accordance with the Trust's data retention periods in Addendum 1 of this policy and Addendum 1 in the Data Privacy Policy-Education**.**

11. Data Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. To the extent that your job requires you to collect or process personal data, this means that you:

- Must ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it;
- Must check the accuracy of any personal data at the point of collection and at regular intervals afterwards; and
- Must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

12. Data Retention

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. The Trust and to the extent that your duties involve the processing of personal data, you must not keep personal data in a form which permits the

identification of the data subject for longer than needed for the legitimate Purposes for which we originally collected it.
The Trust's Data Retention periods, see Addendum 1 for staff data retention periods, are designed to ensure personal data is deleted after a reasonable time, unless a law requires such personal data to be kept for a minimum time.
The Trust and to the extent that your duties involve the processing of personal data, you will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with Addendum 1 of this policy and Addendum 1 of the Data Privacy Policy-Education.

13. General Data Security

The Trust will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We have procedures and technologies in place which are designed to maintain the security of personal data from the point of collection to the point of destruction. In summary, this means that the Trust and our staff must ensure that:

- Only people who are authorised to use the personal data can access it;
- Steps are taken to ensure that people who are authorised to access personal data are not accessing or processing personal data for reasons which are unrelated to their job role;
- Steps are taken to verify the identity of a Data Subject before discussing their personal data with them;
- Personal data is not carried off-site, saved on permitted storage devices which are encrypted and password protected and only when it is legally necessary to do so. Where personal data needs to be carried off-site in paper form, staff must ensure the information is kept safe and secure to avoid any personal data breaches.
- Personal data breaches, or circumstances which might reasonably lead to a personal data breach, are promptly reported; and
- Our security procedures e.g. door entry controls, use of secure locking cupboards, disposal, shredding procedures, the use of encryption, are followed.

The accessing and appropriate use of personal data is something the Academy and Trust takes very seriously. We have an Acceptable Use Agreement which is reviewed at least annually, which all staff sign. Copies are kept on file in the academy.

ICT Acceptable Use Agreements are signed by all Staff/Governors/Pupils/Visitors who will use the school's IT Systems. See the Trust's eSafety Policy.

14. IT Security

All staff must ensure that:

- They have read and understand the policies relating to data privacy and the user acceptance agreement and ask their manager if they are unsure.
- Personal data is stored on the Trust's computer systems instead of individual PCs, laptops, tablet devices, mobile telephones etc;
- Computers and laptops are not left unattended without locking their screens via password controls to prevent unauthorised access;

- Laptops used by staff off our premises (loaned by the trust/academy) and other removable storage devices used to transport work related files, where used for any personal data must be encrypted.
- Administrators with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SIMS learning gateway (SLG) and Learning Platform access are controlled by the Data Protection co-ordinator in the academy, who will ensure access is only given to those staff who require it to undertake their roles
- All data is transferred internally via SIMS or as files which remain stored on the Trust's network or approved cloud storage platform (although may be accessed via the secure Remote Desktop).
- The Trust uses approved sites to securely transfer CTF pupil data files to other establishments.
- Backups are stored securely offsite or in approved, cloud hosted storage.
- Disks are overwritten or physically destroyed prior to recycling where they may have been used for storing personal data.
- Only staff with legitimate reasons are given access to systems and have a unique ID and password.
- Any portable equipment or removable devices such as phones, pen drives or media containing personal data, or connected to trust/academy devices must be encrypted. If in doubt, contact your IT Services team who can advise further.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared photocopiers (multi-function print, fax, scan and copiers) are used.
- Anyone expecting a confidential/sensitive fax should have warned the sender to notify before it is sent.
- When communicating personal data by email, staff should ensure that they only send to people with a right to have the information and they must check that they have the correct email address before sending it.
- Personal data of a sensitive nature or special category data, as defined above, should not be emailed or otherwise transmitted without a password, unless this is absolutely unavoidable.
- Personal data should not be downloaded onto personal computers.
- If the academy has a Mobile Device Management (MDM, e.g. Meraki) system in place, then all academy owned hardware should have this system deployed in order to simplify management and enhance security.

Note: *It is easy to password protect information within Microsoft Office (simply click "Protect Document" from within the file menu in Office 2013) – encryption passwords should be shared by a means other than that by which the document is being transmitted (e.g. for emailed files, phone the recipient to confirm the password). Use a new "one time" password for sharing such information – not one you use to log in to other systems!*

Please refer to the BFET Password Policy for further guidance

You are strongly advised to keep a secure unencrypted copy of such files should it be necessary to access the file in future – files encrypted in this manner *cannot* be accessed without the password *by design*.

15. Bring Your Own Device (BYOD)

Many staff have their own device which they wish to use for Trust purposes (e.g. reading email, checking calendars and potentially storing personal data about pupils). **Even though the device may belong to a member of staff, the data remains the responsibility of the Trust as Data Controller**.

If staff wish to use their own mobile device to process (e.g. record, modify or simply store) any personal data, these devices *must* comply with the following rules:

- The device must be protected by a passcode of at least 4 digits.
- The device must be set to lock automatically after no more than thirty minutes of inactivity.
- No personal data relating to members of the school should be backed up or stored in unapproved "cloud" services such as DropBox, iTunes etc.
- Devices must not be "rooted," "jailbroken," or contain Apps which have been installed from untrusted sources.
- The device must be connected to school email via Exchange/ActiveSync to enable remote wipe.
- The device owner must undertake to notify IT Services immediately that the device is suspected lost or stolen so a remote wipe can be initiated.

Staff should be clear about the implications of the last two points. Should a device be lost or stolen, they are under an obligation to notify IT Services who will immediately send a remote wipe request to the device. This will have the effect of erasing the entire device and any installed removable media cards. Should the device be found subsequently, it will not be possible to restore any data. It is the responsibility of staff to ensure their own data (photos, contacts, etc) are backed up.

Devices owned by staff are subject to Acceptable User Agreement in the eSafety policy for the duration they remain connected to the school network or on school sites.

16. Passwords and their security

- Staff should use their own personal passwords to access computer based services – do not use the accounts of others.
- Staff should ensure that they enter personal passwords each time they logon. Do not include passwords in any automated logon procedures.
- Staff must change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords on paper or in an unprotected file.
- IT Services will not ask you for your password, although it may on occasion be necessary to reset your password to a mutually agreed one. Ensure that all personal passwords that have been mutually agreed are changed once the work is complete.

- Passwords must contain a minimum of six characters and be difficult to guess.
- User ID and passwords for staff and pupils who have left the academy are disabled once the period of employment has ended – you will not be able to access files or emails after this time.
- Do not share your password with others.
- If a member of staff thinks that their password may have been compromised or someone else has become aware of it, change your password immediately and report your concerns to IT Services.
- If staff become aware of a security breach, please notify IT Services immediately.

Please refer to the Password Policy for further information.

17. Remote Access

The Trust provides some remote access functionality ("Terminal services," "Remote Desktop," "CITRIX," etc) which should always be used in preference to other means of accessing information.

- Staff are responsible for all activity via the remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- This policy and the eSafety policy apply to all activity undertaken whilst remote access is used.

18. Staff Training

As part of our commitment to data security, all staff will receive training on our data privacy policies and procedures as part of their induction and this will be refreshed at regular intervals thereafter as part of whole school training once per year..

19. Mandatory Data Breach Reporting

Under the GDPR the Trust has certain obligation to mandatorily report personal data breaches. A personal data breach (**personal data breach**) is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
There are two levels of mandatory reporting obligation, which depend upon the level of risk arising from the personal data breach:

Mandatory Reporting Obligation	Details
Report to Information Commissioner must be made ASAP (at latest within 72 hours of becoming aware of the Personal data Breach). **Only the Data Protection Officer can report a breach to the ICO**	If the personal data breach is likely to result in **a risk** to data subject's rights and freedoms. Examples: • Report: – e-mailing details of an SEN pupil's assessments to the wrong external e-mail address; – a ransomware attack which results in all personal data being encrypted and no back-ups are available; • Do not report: – loss of a staff telephone list which is publically accessible;

	– loss of a securely encrypted mobile device, provided the encryption key remains within our secure possession and this is not the sole copy of the Personal data.
Notify data subject "without undue delay" and "as soon as reasonably feasible".	If a personal data breach poses a **high risk** to a data subject, then it must be directly reported to them as well as the Information Commissioner unless an exception applies. High risk situations are likely to include the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation or financial loss. Examples of high risk personal data Breaches: • A cyber-attack leads to personal data being infiltrated from our server; • We suffer a ransomware attack which results in all personal data being encrypted. No back-ups are available and the data cannot be restored; and There are some limited exceptions to the mandatory requirement to report a Personal data Breach to the Data Subject.

Failure to make the relevant mandatory personal data breach report may lead to a financial sanction against the Trust.
It is the responsibility of all Staff to **immediately** i.e. within 24 hours, report any personal data breach which comes to their attention (whether it involves you or any other member of Staff, whether subordinate or senior to you), or circumstances which might reasonably be interpreted as a personal data breach, or which could lead to a personal data breach to the Data Protection Officer dataprotection@bfet.uk.

20. The Trust's Data Protection Officer (DPO) and academies' data protection co-ordinator contacts

The Trust has appointed a Data Protection Officer for GDPR purposes, who has overall responsibility for the Trust's policies and procedures relating to data privacy. In addition, each school has identified a Data Protection co-ordinator. The co-ordinator for your school is:
Nicola Carson, Assistant Vice Principal

The Data Protection co-ordinator should be your first point of contact in the following situations:

- If you have any concerns, or require clarification, about your or the Trust's obligations regarding data privacy;
- If you have any feedback or suggestions about how the Trust can improve its data privacy and/or data security procedures;
- If you are introducing any new technologies or propose to introduce a new way of processing personal information which could pose a high risk to individuals and need to undertake a data privacy impact assessment.

The Data Protection Officer should be your first point of contact in the following situations:

- If you receive a request from a data subject seeking to:
  - Access their Personal data (see "Subject Access Requests" above); or
  - Exercise any of their other rights as a Data Subject (see "What rights do data subject's have?" above), such as to withdraw their consent to processing;
- If you become aware of any member of Staff:
  - Abusing their role to access personal data for non-permitted reasons;
  - Processing personal data in a manner which is inconsistent with this Data Privacy Policy;
  - Committing a breach of our Data Retention schedule.
- If you, or any other member of Staff (whether subordinate or senior to you), are involved in a personal data breach, or circumstances which might reasonably be interpreted as a personal data breach, or which could lead to a personal data breach (see "Mandatory Data Breach Reporting" above).

Our Data Protection Officer is: Lynette Beckett
Her contact details are:
Telephone: 0161 941 5681. Email: dataprotection@bfet.uk.
Postal: The Lodge House, Cavendish road, Bowdon, Altrincham, Cheshire, WA14 2NJ.

Further Information

The Information Commissioner' website provides various help and support. As follows:
https://ico.org.uk/for-organisations/education/

Addendum 1- Personal data Retention periods

Staff

Basic description	Statutory Provisions that may apply	Retention period	Action at the end of the retention period
All records leading up to the appointment of a member of staff, including other applications and their records	We may need to defend a claim for discrimination in our selection processes	6 months following the appointment The records relating to the successful candidate are held on their staff file	Secure in school disposal
Pre-employment vetting –criminal records data captured as part of the application process (separate sheet from the application form)	Keeping Children Safe in Education, September 2016 and subsequent updated versions	For unsuccessful candidates-destroy immediately For successful candidates, hold on staff file until DBS clearance is received and then destroy	Secure in school disposal
Pre-employment vetting –DBS clearance certificate and number. (original to be seen and on-line notification received by academy to be signed to say original certificate seen, by whom and dated)	Keeping children Safe in Education September 2016 and subsequent updated versions	Certificate to be immediately returned to the member of staff DBS number to be retained on the Single Central Record and the online confirmation (signed etc) held on the staff file. These are held as part of the staff file, see below	Returned to member of staff
Pre-employment vetting - Disqualification by Association. *Only applies to posts in some schools* (Completed form)	Disqualification under the Childcare Act 2006 and subsequent guidance	Held on staff file	
Pre-employment vetting-references	Keeping children Safe in Education September 2016 and subsequent updated versions	Held on staff file see below	
Pre-employment vetting- Evidence of the Right to Work in the UK.	An Employers Guide to right to work checks (Home Office 12 July 2016)	Held on staff file see below	

(Photocopy, signed to say original seen, by whom and dated)			
Staff file, containing recruitment documents, contractual paperwork, occupational health reports relating to employment decisions, qualification certificates including QTS, DBS online clearance confirmation,	Limitation Act 1980 (section 2)	Termination of employment + 6 years	
Staff file for 'Officers' e.g. CEO	Limitation Act 1980 (Section 2)	6 years from date of resignation or termination	
Time sheets	Working Time Regulations 1998	Current year + 6 years	Secure in school disposal
Appraisal records	Education (School Teachers' Appraisal) (England) Regulations 2012 (the Appraisal Regulations). Teachers and school leaders only	Current year + 6 years	Secure disposal
Medical certificates/fit notes, linked to the payment of sick pay	HM Government - Statutory Sick Pay (SSP): employer guide	Current year + 3 years	Secure in school disposal
Disciplinary/capability/Absence formal warning records (including the file of evidence)	Some cases: Keeping children Safe in Education September 2016 and subsequent updated versions	Date of the warning + 6 months Unless the case relates to Safeguarding in which case the case file should be retained 10 years after the allegation	Secure in school disposal and must be shredded
Maternity leave, parental leave, redundancy letters, notifications	Employment Rights Act 1996 and Equality Act 2010	Held on staff file see above	Secure in school disposal

PART TWO-PUPILS, PARENTS AND CARERS DATA SECURITY POLICY

DATA PRIVACY POLICY -EDUCATION

Bright Futures Educational Trust's (BFET or the Trust) Strategy underpins all aspects of this policy and the way in which it will be applied. These elements are:

- Our vision, the best ***for*** everyone and the best ***from*** everyone;
- Two of our values; **Integrity**: We do the right things for the right reasons and **Passion**: We take responsibility, work hard and have high aspirations;
- Two of our commitments: **Effective Communication** and **Strong Governance and Accountability.**

What is the Policy for?

This policy sets out the duties of Bright Futures Educational Trust ("the **Trust**") under General Data Protection Regulation ("GDPR"), the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. The policy details the responsible bodies/person for compliance and the procedures that will be applied.
By Trust we mean, all academies in the Trust and the head office of the Trust

Who is the Policy for?

Part Two of this policy is for pupils and parents/cares to understand how their personal data will be handled. It is also for staff to understand their responsibilities in handling the personal data of pupils, parents and carers. It is published on our website.

Part One of this policy is for the attention of anyone who is employed by, provides a service to, or volunteers to work at the Trust and its academies. This includes governors and trustees.

About this policy

Our Trust processes personal information relating to pupils, staff and visitors, and, therefore, is a Controller.

The Trust is registered as a Controller with the Information Commissioner's Office and renews this registration annually. The Trust's registration number is: ZA023935.

During the course of its activities the Trust will process personal data (which may be held on paper, electronically, or otherwise) about the Trust's staff (including temporary staff), agency workers, volunteers, pupils, their parents, or carers, and other individuals (including suppliers and governors and trustees).
The Trust Board also complies with ICO and DfE Guidance applicable from time to time.

Definitions

The definitions in this paragraph apply in this policy.

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identifiable
Special categories of personal data (formerly sensitive)	Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation and sex life • Biometric or genetic data
Criminal conviction data	Data relating to criminal convictions and offences.
Processing	This has a very wide definition and includes the following operations with personal data: collection, recording, organisation, structuring, storage, adaption, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and/or destruction.
Data subject	The living individual whose personal data is held or processed
Controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Processor	A person or organisation that processes personal data on behalf of a Controller.

Policy Standards

1. Data protection and educational records

The Trust will comply with the six data protection principles in the GDPR, which require that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purpose for which it is maintained;
- accurate and, where necessary, kept up to date;
- not be kept in a form which permits identification for longer than is necessary for the purpose(s) for which it is processed; and
- processed in a manner that ensures appropriate security of the data.

2. Fair, lawful and transparent processing

- The Trust will only process personal data where it is based one or more of the conditions specified in the GDPR. The most common conditions we rely on to process personal data are:

Conditions for Processing which we commonly rely on	
Personal Data	**Special Category Personal Data & Criminal Convictions Data**
• The data subject has given consent to the processing for one or more specific purposes; • Processing is necessary for entering or performing a contract with the data subject; • Processing is necessary for compliance with a legal obligation to which the controller is subject; • Processing is necessary to protect the vital interests of the data subject; • Processing is necessary in order for the controller to perform a task in the public interest or for the controller's official functions, and the task or function has a clear basis in law; or • Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party where this does not relate to our "core function" of providing education.	• The data subject has given explicit consent to the processing for one or more specific purposes; • Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; • Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent; • Processing relates to personal data which are manifestly made public by the data subject;

	• Processing is necessary for reasons of substantial public interest; • Processing is necessary for the establishment, exercise or defence of legal claims; or • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (however this condition is limited in its use to certain authorised professions as explained at Article 9(3) GDPR).

- The full list of conditions is set out in Articles 6 and 9 of the GDPR and the Trust may in some circumstances rely on other conditions set out in the GDPR or Data Protection Act 2018 to justify the processing of personal data or special category personal data. The ICO's website also has further information about the lawful conditions for processing.

3. How the Trust is likely to use personal data.

The Trust will process data about **pupils** for the following (non-exhaustive) purposes:

- for legal and administrative purposes;
- to provide education and discharge the **Trust**'s duty of care as an education provider;
- to provide pupils with a safe and secure environment and pastoral care;
- to provide activities including school trips, activity and after-school clubs;
- to support pupil learning;
- to monitor and report on pupil progress
- to provide academic and examination references;
- to enable the **Trust** to meet the it's legal obligations under relevant legislation and Department for Education (DfE) Guidance in force from time to time;
- to maintain educational records;
- to monitor attendance;
- to maintain health and safety records;
- to collect opinions about ability and achievements;
- to obtain and retain details about personal / home life where this is relevant to provision of education to a data subject; and,
- to share information with other agencies when required.

3.1. Publishing Student's Images and Work

On a student's entry to the academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site, or social media feeds.

- In the academy prospectus and other printed publications that the academy or Trust may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the academy's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the academy.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Parents/ carers may withdraw permission, in writing, at any time, or by other means provided by the academy (e.g. using the Data Collection system in SLG). We request consent to be given by both parents/carers in order for it to be deemed valid, wherever possible. The law establishes that a child in England must provide their consent from the age of 12/13 if they have the ability to understand the nature of the request and what the consequences of providing it will be. The Trust respects the views of parents and carers so also seeks their approval for use of images. However, if the consent differs after the school has tried to reach an agreement with all parties and the child is deemed to be competent by the school, then the child's view will prevail. When obtaining consent, we will set out that we wish to use a child's images for the duration of their time with us and for 6 years after they have left.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Where pupils' full names are to be published (e.g. to celebrate examination results), parents/carers will be given opportunity to opt out.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed from an up-to-date list.

3.2. Storage of Images

- Images / films of children are stored on the Trust/school's secure network.
- CCTV is used for security purposes. We do not seek consent for the use of CCTV images as these are collected in accordance with our public task to keep children in our care safe.
- Rights of access to this material are restricted to the staff and pupils within the confines of the school network, or via secure Remote Desktop connections.
- Images and videos of pupils recorded or stored on equipment (e.g. trips, mementoes of previous classes) will be in line with appropriate legislation and the Teachers' Standards.
- The IRIS system may be used to record lessons for staff appraisal and reflection. Since the videos are stored in an encrypted form, cannot be downloaded and may only be shared with other staff at school, explicit permission need not be sought (similar to CCTV).

3.3. Webcams

- Webcams in school are only ever used for specific learning purposes, e.g. monitoring science experiments such as eggs hatching or video conferencing.

- Misuse of the webcam by any member of the community will result in investigation and sanctions.
- Consent for publication of images is assumed to extend to use of webcams.

3.4. Use of Biometric Data

Any biometric information (defined as: "*personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements"*) must be stored in accordance with Data Protection legislation. However, if that information is also used for an automated biometric recognition system (e.g. fingerprint recognition for pre-payment dinner money), schools must also comply with sections 26-28 of the Protections of Freedoms Act 2012. This requires that we obtain parental consent for all pupils up to the age of 18. All pupils are also entitled to refuse to have their fingerprint used for this system regardless of whether a parent consents. If that is the case, alternative payment methods for our cashless catering services will have to be considered.

In essence, Academies must notify parents (or carers) of the intention to use biometric data, giving parents and pupils the right to opt out should they wish. Alternatives (e.g. a card payment system) must be provided for pupils who choose to opt out.

3.5. Special Category Personal Data

The Trust may process special category personal data relating to pupils including, as appropriate:

- information about pupil's physical or mental health or condition (including but not limited to allergies and regular medications) in order to discharge the **Trust**'s duty of care, provide non-emergency and emergency medical assistance and for special educational needs provision;
- provide applicable provision under an Education Health and Care Plan/Statement of Special Educational Needs;
- the pupil's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation or to ensure that religious or similar beliefs are respected;
- share in a multi-professional team around a child; and/or,
- in order to comply with other legal requirements and obligations to third parties.

The Trust may process data about parents, carers and other individuals (including suppliers and governors) for the purpose of:

- providing education to pupils;
- reporting on pupil progress;
- maintaining emergency contact details in order to discharge the Trust's duty of care as an education provider;
- organise training courses;
- obtain and retain details about personal / home life where this is relevant to provision of education to pupils; and
- discharge obligations under safeguarding and other relevant legislation.

- It is very unlikely that the Trust will process sensitive personal data relating to parents, carers and other individuals (including suppliers, governors and trustees). However, where this may be necessary, it may include, as appropriate:
- the parent, carer or other individual's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- when there is relevant medical information needed for health and safety purposes including allergy information; and/or,
- in order to comply with other legal requirements and obligations to third parties.

4. Processing for specified, explicit and legitimate purposes

- The Trust will only process personal data for the specific, explicit and legitimate purpose or purposes notified to data subjects and will not be further processed in any manner incompatible with that purpose or purposes.

5. Adequate, relevant and limited to what is necessary

- Personal data will only be processed to the extent that it is relevant and necessary for the specific purposes notified to the data subject.

6. Accurate and when necessary, kept up to date

- The Trust will keep the personal data the Trust stores about a data subject accurate and when necessary, kept up to date. Data that is inaccurate or out of date will be corrected or deleted without delay. Data subjects should notify the Trust if any personal details change or if the data subject becomes aware of any inaccuracies in the personal data the Trust hold about him/her.

7. Data retention

- The Trust will not keep personal data for longer than is necessary for the purpose for which it is processed. Sometimes we are required by law to retain information for a specified period. After the retention period has lapsed, and there is no other legitimate reason to retain the information, the Trust will take steps to destroy it so that it is no longer processing it.

- The table in Addendum 1 specifies the retention period of personal data relating to pupils, parents, carers and other individuals (including suppliers, governors and trustees). Retention periods for staff/workers' data is contained in the Data Privacy Policy-Staff.

8. Data security

The Trust will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Appropriate measures include:

- Appropriate levels of authority being given to staff members where access to personal data is required;
- Personal data is stored on the academy's central computer system instead of individual PCs, laptops, tablet devices, mobile telephones etc;
- Computers and laptops are not left unattended without locking their screens via password controls to prevent unauthorised access;

- Personal Data is not carried off-site, unless it is on permitted storage devices which are encrypted and password protected or when it is legally necessary to do so. Where Personal Data needs to be carried off-site in paper form, staff must follow any guidance issued from time to time to ensure the information is kept safe and secure to avoid any personal data breaches.

Our key security procedures are as follows:

- Lockable cabinets, drawers and cupboards;
- Lockable offices
- Clear desk policy when leaving a desk or leaving the office for the day, unless it is locked and no access can be gained by other staff including cleaners
- Laptop and other mobile device / document encryption;
- Laptop and other mobile device / document password protection;
- Regular back-ups of the Academy/Trust's servers;
- Sharing personal data internally (i.e. from person to person in the academy/trust is only done in accordance with the Data protection Principles in Section 1 above)
- Where personal data is shared by email, whenever practicable, it will be attached to the email as an encrypted document.
- ICT Acceptable Use Agreements are signed by all staff/Governors/Pupils/Visitors who will use the school's IT Systems. See our E-Safety policy.
- Servers are locked in a secure server room managed by DBS-checked staff
- Backups are stored securely offsite or in approved, cloud hosted storage and subject to contractual agreements to ensure information provided is processed in a secure and legally compliant way.
- We use recommended disposal firms to securely destroy drives where personal data may have been stored.
- Papers are shredded for secure disposal
- Disks are overwritten or physically destroyed prior to recycling where they may have been used for storing personal data.

9. Sharing information with third parties

- The Trust has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. The Trust will only transfer personal data to a third party the third party agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

- Where the Trust uses a third party processor to process personal data on its behalf, it will have in place a written agreement with each processor which meets the requirements of Article 28 GDPR.

- The **Trust** routinely shares pupil information with:
  - schools that the pupil attends after leaving us;
  - our local authority/councils
  - social services/ children's services where there are safeguarding concerns;
  - the Department for Education (DfE);

  - any appointed processor, who analyses pupil data on our behalf to provide academy and trust wide management information.
  - Feeder schools

- The Trust does not share information about pupils with anyone without consent unless the law and our policies allow us to do so.

- The Trust will share information with multiple agencies which are formed as a team around a child or young person. These agencies will be controllers and be subject to the same obligations under data protection law as the Trust is. The Trust will be under a legal obligation to share most of the information that is relevant to the multi-agency team or will be required to do so in the performance of the school's public task.

- The Trust is also legally required to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education (DfE), so that they are able to meet their statutory obligations. This data sharing underpins school funding and educational attainment policy and monitoring.

- The Trust is required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

- Once pupils reach the age of 13, the Trust also passes pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 14 Education and Skills Act 2008 (to enable the local authority to meet the requirements of section 507B of the Education Act 1996).
  This enables them to provide services as follows:
  - youth support services
  - careers advisers

- A parent or carer can request that certain information is not passed to their local authority or provider of youth support services by informing the Trust of their instruction. This right is transferred to the child / pupil once he/she reaches the age 16.

- The Trust will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
  This enables them to provide services as follows:
  - post-16 education and training providers
  - youth support services
  - careers advisers

  For more information about services for young people and how personal information will be used for these, please visit the relevant local authority website.
- The Trust will only transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country ensures an adequate level of protection for the individuals' rights and freedoms;
- The individual has given consent;
- The transfer is necessary for one of the conditions set out in the GDPR (e.g. for the performance of a contract between us and the individual, or to protect the vital interests of the individual);
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or
- The transfer is authorised by the Information Commissioner where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

10. Processing in line with subject access rights

Individuals have the following rights which they can exercise by contacting the Trust's DPO:

Right	What it is for?
To be informed	This policy and any accompanying privacy notice sets out the information about how the Trust processes personal data about pupils and parents. It will be reviewed annually to ensure we are as transparent as possible about the personal data that we process.
Rectification	If the Trust is processing an inaccurate record about an individual they have the right to request that we review it and rectify it so as to make it accurate. This only extends to factual information being processed about an individual.
Erasure	If the Trust has no compelling reason to process data about an individual, there is a right for the data to be erased and processed no further. This is not an absolute right and the Trust will consider requests on a case by case basis.
Restrict processing	This right complements the right to rectification. Processing of personal data can be restricted whilst the Trust considers if any records are inaccurate or an objection has been raised about the personal data that it is processing.
Data portability	This enables individuals to seek (in certain circumstances) for information which they have provided to the Trust and which is being processed through automated means based on their consent or for the performance of a contract to have it transmitted in machine readable form to the individual or a third party.

	It is unlikely that this right will apply to the information which the Trust processes about parents and pupils. It could extend to images processed by the Trust when the lawful condition relied upon is consent.
To object	When the Trust is processing personal data about pupil's and parents for the performance of a task in the public interest those individuals have the right to object to processing. The Trust will consider any objection but may be able to demonstrate a legitimate ground to continue to process the personal data concerned.
To know about any automated decision making and profiling	The Trust will inform individuals when it uses any automated decision making processes. Individuals are entitled to request that automated decisions involving them are reviewed by human intervention. We profile pupils' performance to ensure that the school can meet their educational needs.

11. Subject access requests

- Under the data protection law, individuals have a right to request access to information the Trust holds about them. This is known as a subject access request. For our Secondary schools this means for a parent to make a subject access request on behalf of a pupils, the pupil must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

  For our Primary/early years' establishments, parents can exercise a pupil's right of access on their behalf due to their age and lack of understanding of the rights afforded over their personal information.

  For those pupils with special educational needs we will need to consider their level of competency to consider if they are able to exercise their data subject rights on their own behalf, or if their parent or carer must do this.

- Subject access requests from 'competent' children age 12/13, or from parents of children who are not 'competent' or under age 12, should be submitted in writing, either by letter, or email to the Trust's Data Protection Officer ("DPO"). The e-mail address of the DPO is dataprotection@bfet.uk. Requests should include:
  - The pupil's name
  - A correspondence address
  - A contact number and email address
  - Details about the information requested to assist the school to confirm if the personal data is being processed and to provide a copy within the time period afforded

- The Trust will not reveal the following information in response to subject access requests:
  - Information that might cause serious harm to the physical or mental health of the pupil or another individual
  - Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
  - Information contained in adoption and parental order records
  - Certain information given to a court in proceedings concerning the child
  - Third party personal data where there is no consent to disclose this in response to a subject access request and it would not be reasonable in the circumstances to do so.

- Once the identity of the requestor is verified, the information will be provided within 30 calendar days. If the request is complex, numerous or arrives during the school holidays and records cannot be accessed the Trust has the right to determine that up to a further 2 months is required to respond to a subject access request. The DPO will write to the data subject within a month of their written request to set out the reasons why the time is being extended.

- If the request is determined to be manifestly unfounded or excessive, the Trust has the right to either charge a fee to reflect the administrative costs of providing the response or to refuse to provide a response. In the event that such a determination is made, the DPO will write to set out the Trust's reasons within a month of the written request being made.

12. Data Protection Officer ("DPO")

The **Trust** has appointed a Data Protection Officer who has overall responsibility for the T**rust's** policies and procedures relating to data privacy. The Data Protection Officer should be the first point of contact for individuals in the following situations:
Where individuals have any concerns, or require clarification, about the **Trust**'s obligations regarding data privacy and how we handle data;

- To report a data breach or potential data breach;
- Where an individual has any feedback or suggestions about how the **Trust** can improve its data privacy and/or security procedures;
- Where an individual wishes to make a subject access request or exercise one of their other data privacy rights.

Our Data Protection Officer is: Lynette Beckett
Her contact details are:
Telephone: 0161 941 5681. Email: dataprotection@bfet.uk.
Postal: The Lodge House, Cavendish road, Bowdon, Altrincham, Cheshire, WA14 2NJ.

13. Breaches of data protection and complaints

- If an individual considers that this policy has not been followed in respect of personal data about a data subject he/she should raise the matter with the Data Protection Officer in the first instance.
- Compliance with data protection law is regulated by the Information Commissioner. In the event that you are not satisfied with the way in which the Trust is processing your personal data and you are not content with the response from our DPO, you have the right to refer

your concerns to the Information Commissioner's Office ("ICO"). You can contact the ICO at https://ico.org.uk/concerns/ or via its helpline number which is available on its website.

Addendum 1- Personal Data Retention periods. Personal Data types for pupils, parents/carers held by the Trust/Local Governing Body/Principal and senior leadership team in academies

Basic description	Statutory Provisions that may apply	Retention period	Action at the end of the retention period
Papers and minutes that contain reference to named pupils or parents/carers	Education Act 202, section3.3 Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 S1 2002 No 1171	6 years, with a review of the personal data held after 3 years	Secure disposal
Admissions	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and appeals panels December 2014	Data of admission/decline/resolution of an appeal + 1 year	Secure disposal
Admissions register	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Permanently	Not applicable
Pupil's educational record and file – primary (including internal and external examination results)	The Education (Pupil Information) (England) Regulations 2005 S1 No 1437	Whilst the child is in school	The file is then transferred when the pupil moves to another primary school/secondary/pupil referral unit. In the case of a pupil death, transfer to an independent school, transfers to home schooling or leaves the country; file is transferred to the Local Authority to be retained in accordance with their policy.
Pupil's educational record and file– secondary (including internal and external examination results)	The Education (Pupil Information) (England) Regulations 2005 S1 No 1437 Limitation Act 1980 (Section 2)	Until the child is 25 years of age	Secure disposal All uncollected examination certificates should be returned to the examination board

Basic description	Statutory Provisions that may apply	Retention period	Action at the end of the retention period
Child Protection information held on pupil file	"Keeping Children Safe in Education September 2016"- Statutory Guidance, as updated from time to time "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children –March 2015" and as updated from time to time	Retained for the period of the pupil file, in a sealed envelope	Secure disposal, and must be shredded
Child Protection information held in separate files	Keeping Children Safe in Education- Statutory Guidance, as updated from time to time "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children –March 2015" and as updated from time to time	Until the child is 25 years of age.	Secure disposal, and must be shredded
Accident Reports		Until the child is 25 years of age	Secure disposal
Student grant/bursaries information		6 years	Secure disposal
Pupil premium/free school meals		6 years	Secure disposal
Attendance registers	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	3 years from the date of the entry	Secure disposal
Correspondence relating to authorised absence	Education Act 1996 Section 7	Current academic year +2 years	Secure disposal
Special Educational Needs files, reviews and individual education plans	Limitation Act 1980 (Section 2)	Until the child is 25 years of age	Secure disposal
Statement maintained under Section 234 of the Education Act 1990 and any amendments made to the statement	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Until the child is 25 *years of age* (usually held as part of the pupil file)	Secure disposal unless the document is subject to legal hold

Basic description	Statutory Provisions that may apply	Retention period	Action at the end of the retention period
Advice and information provided to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 2	Until the child is 25 years of age (usually held as part of the pupil file)	Secure disposal unless the document is subject to legal hold
Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 14	Until the child is 25 years of age (usually held as part of the pupil file)	Secure disposal unless the document is subject to legal hold
Parental consent forms for school trips where there has been no major incident		Conclusion of the trip	Secure disposal
Parental consent forms for school trips where there has been a major incident	Limitation Act 1980 (Section2)	Until the child is 25 years of age (to show that rules had been followed)	Secure disposal
Visitors Books and signing in sheets		6 years	Secure disposal