Bright Futures
EDUCATIONAL TRUST

Data Protection Policy

Including guidance on:

The Data Protection Act, 1998

The Freedom of Information Act, 2000

Protecting and educating staff and students in the safe use of technology

Ensuring the safety and fair processing of all data for which we are responsible as a data controller

This is a Trust-Wide Policy. It applies to all the schools within the Trust and the central Trust office.

Date of Policy Approval:	**12 January 2016**
Owner of Policy:	**Head of IT**
Authorised By:	**BFET Operations Board**
Policy Review Date:	**Winter 2017/2018**
Distribution:	**All Trust Staff** **All Members/Directors/ Governors** **Consultants working on behalf of the Trust** **Trust/Academy Websites**

DATA PROTECTION POLICY

The vision of Bright Futures Educational Trust is to create a world class education to enable every young person to reach their full potential and in particular, their full academic potential. In order to achieve this everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

What is the Policy for?

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners.

We have three classifications of data and documents:

Classification	Brief Description
Unclassified (assume if unmarked)	Document or dataset contains no sensitive or personally identifiable information.
Protect	Document or dataset containing sensitive or personally identifiable information, including class lists which contain data about the individuals (such as UPN, marks or grades).
Restricted	Document or dataset containing highly sensitive or personally identifiable information, including class lists which contain particularly delicate information about the individuals (such as religion, sexuality or SEND details).

All documents containing personal information should be marked as “Protect” or “Restricted” and thereafter treated as outlined in this document.
(Much of the content of this document is based on “Network Manager Guidance for Schools on Data Security Feb 2012” from http://www.thegrid.org.uk/info/dataprotection/index.shtml)

Who is the Policy for?

The Policy applies to all employed staff and other contractors/consultants/agency staff who are working in any school in the Trust.

Policy Standards

General Principles

Dos and Don'ts

Do:

- Make sure you have read the Data Protection and eSafety policies – ask if there is anything of which you are unsure.
- Raise any concerns to the relevant IAO (see local addenda for a list).
- Be wary of unsolicited emails, particularly if they contain links or attachments.
- Follow the Acceptable Use Agreement for IT use (in the eSafety Policy)
- Choose passwords that are "strong," easy for you to remember and hard for anyone else to guess.
- Lock any computer that you're stepping away from, even momentarily.
- Log out of any computer when you've finished using it.
- Use secure methods (such as Remote Desktop) to access data and files from your academy.
- Have any school laptop you use for storing personal data encrypted by your IT Services team.
- Make sure all sensitive information (such as planners) is away when not in use.

Don't:

- Email sensitive or personally identifiable data as attachments unless unavoidable – wherever possible, strong encryption should be used.
- Put sensitive or personally identifiable data onto removable media (such as memory sticks or CDs), unencrypted laptops, or your own machines.
- Write passwords down, or share them with anyone else.
- Leave logged on machines unattended.
- Leave sensitive or personally identifiable data visible and unattended – this includes your planner.
- Display sensitive or personally identifiable data on screens which may be seen by other people.

Summary of the Data Protection Act

The Data Protection Act (revised 1998) enshrines 8 principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   a. At least one of the conditions in Schedule 2 is met *(i.e. the processing is lawful, necessary or the subject has given permission, etc.)*.
   b. In the case of sensitive personal data *(e.g. race or ethnicity, physical or mental health details, trade union membership)*, at least one of the conditions in Schedule 3 is also met *(i.e. explicit permission has be sought, etc.)*.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Further information on the act and these principles can be obtained from:

https://ico.org.uk/for-organisations/guide-to-data-protection/

A few definitions:

Term	Brief definition
Controller	An individual or organisation who determines what personal data is processed, and how.
Data	Information which can be stored, known, or sent in any format (not *just* electronic data – paper files are included too).
Personal	Data which relates to a living person which can be used to identify that person (e.g. it contains their name or email address) – or identify the person if combined with other information held by the controller (e.g. it contains their admission number).
Processing	Collecting, recording, sending, altering or destroying data.
Processor	Another individual or organisation who processes personal data on behalf on the controller (e.g. a contractor).
Sensitive	Data which contains information about an individual's race, ethnicity, sexual orientation, physical or mental conditions or trade union membership, etc.
Subject	The person to whom personal data relates.

In practice the act means that academies and the Trust must ensure:

1. We have legitimate grounds for holding the data that we process it in a way that won't have adverse effects and we're transparent about the data we collect and what we use it for.

2. We're clear about why we need the data and what we're going to use it for, that we publish a "privacy notice" explaining this, we notify the Information Commissioner's Office of the type of data we hold and any new uses of the data are fair.

3. The data we hold is sufficient for the purpose, but we hold no more than we need.

4. We take reasonable steps to ensure the data is accurate, and updated when necessary.

5. We consider how long we keep the data and delete it securely when it's no longer needed.

6. We uphold the subject's rights to:
   a. Get copies of the information we hold about them ("Subject Access Requests").
   b. Object to the processing of the data.
   c. Opt out of direct marketing.
   d. Object to automated decisions.
   e. Have their data corrected or erased.
   f. Potentially claim damages in the event of a breach of the Act.

7. That security and policy is in place to protect the data we hold and stop it being lost or obtained by someone outside of the organisation who shouldn't have it and that we have procedures in place should something go wrong.

8. That we ensure the data will be subject to similar regulations should it be transferred abroad.

Specific Standards

General Data Security

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

ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors who will use the school's IT Systems.

Guidance documents (i.e. this Policy) are issued to all members of the school who have access to sensitive or personal data.

Protect and Restricted material must be encrypted if the material is to be removed from the academy.

- The use of unencrypted media for the transfer of Protected and Restricted materials is not permitted.
- At this academy we use approved sites to securely transfer CTF pupil data files to other establishments.

All data is transferred internally via SIMS or as files which remain stored on the academy network or approved cloud storage platform (although may be accessed via the secure Remote Desktop).

Protect and Restricted material must be kept out of sight, ideally held in a lockable room, storage area, drawer or cabinet if in an un-encrypted format (such as paper) when not in use.

- We store such material in lockable desk drawers or behind locked staffroom doors.
- Servers are locked in a secure server room managed by DBS-checked staff.
- Backups are stored securely offsite or in approved, cloud hosted storage.
- Disposal: Protect and Restricted material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.
- We use recommended disposal firms to securely destroy drives where personal data may have been stored.
- At this academy paper based sensitive information is shredded, using cross cut shredders.
- Disks are overwritten or physically destroyed prior to recycling where they may have been used for storing personal data.
- Laptops used by staff at home (loaned by the academy) where used for any protected data will be encrypted.
- Domain Administrators with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access are controlled by the SIRO.

Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation and training will be provided to keep staff informed.

IT Security

- The academy gives relevant staff access to its Management Information System, with a unique ID and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing academy data, outlined in this policy together with the eSafety policy and AUA.
- Staff have been issued with the relevant guidance documents and the ICT Acceptable Use Agreement.
- Staff keep all academy related data secure. This includes all personal, sensitive, confidential or classified data.
- Any portable equipment or media containing sensitive data 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.
- Protected information (e.g. class lists) should not be included in internal email attachments since these attachments will usually be downloaded in order to be read – instead the contents should be included in the body of the email which is only resident on the viewer's machine for as long as the email is displayed.

- Sensitive or restricted information should not be emailed or otherwise transmitted unencrypted unless this is unavoidable.
- When conducting due diligence studies on potential contractors or suppliers, consideration should be made of how the contractor will act as a potential data processor (e.g. how will data be transferred or received?).
- Protected or restricted information should not be downloaded onto personal computers.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Ensure hard copies of data are securely stored and disposed of after use

It is easy to encrypt 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!

You are strongly advised to keep an 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*.

Bring Your Own Device (BYOD)

Many staff have their own device which they wish to use for academy purposes (e.g. reading email, checking calendars and potentially storing personal data about students). **Even though the device may belong to a member of staff, the data remains the responsibility of the Academy 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 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 AUA in the eSafety policy for the duration they remain connected to the school network or on school sites.

School Owned Devices

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.

Staff Responsibilities

Although these two roles are explicitly identified, **the handling of secured data is everyone's responsibility**. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The Senior Information Risk Owner, or SIRO, is a member of the senior management team who is familiar with information risks and the school's response and has the following responsibilities:

- They own the information risk policy (strategies in place to identify and manage risks associated with information breaches) and risk assessment.
- They appoint or identify the Information Asset Owners (IAOs).

The SIRO for this academy is specified in the local addenda.

Academies should work to develop and maintain a list of information assets, included in the local addenda. These include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Any additions to the list or requests for clarification should be forwarded to the SIRO.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the SIRO.

It is the responsibility of all staff to remain vigilant against the loss or unfair processing of data.

Passwords and Password Security

1. Passwords

- Always use your own personal passwords to access computer based services – do not use the accounts of others.
- Make sure you enter your personal passwords each time you 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 students 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 you think your password may have been compromised or someone else has become aware of your password change your password immediately and report your concerns to IT Services.**
- **If you become aware of a security breach, please notify IT Services immediately.**

2. Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the academy's policies on e-safety and Data Security.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of academy networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.
- All networked workstations have an automatic screen saver (password protected) set to 15 minutes.
- However, all staff are advised to lock their workstation when leaving their PC unattended – this can be done by pressing "Windows" key and "L" at the same time on Windows machines – your password will be required to log in again.
- Do not leave computers locked when someone else may require access, particularly computers in classrooms – log out completely in this case.

Remote Access

Some academies provide remote access functionality ("Terminal services," "Remote Desktop," "CITRIX," etc) which should always be used in preference to other means of accessing information.

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- Never write down your password – pick a password which is easy for you to remember but hard for someone else to guess.
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from an external environment (e.g. at home).
- Do not use the remote access facility as a means to download protected or restricted information (including class lists).

Action in the Event of a Data Breach

In the event of a data breach, there are four main areas to be addressed:

- Containment and recovery
- Assessment of ongoing risk

- Notification of breach
- Evaluation and response

1. Containment and Recovery

The SIRO should take the lead in assessing what information has been lost or otherwise compromised, and determine who needs to be notified. The SIRO will then determine, with appropriate staff, what steps to take to contain the breach and recover the data. If appropriate, the police should be informed (e.g. theft of laptop).

2. Assessment of Ongoing Risk

An assessment needs to be made of the likely impact of the loss of data, depending on the type of data involved, the sensitivity of the data, to whom the data belongs and how much data has been lost. An assessment should also be made of any potential harm (e.g. financial, emotional) which may come to the individuals whose data has been lost, or harm to the reputation of the academy or Trust.

3. Notification of Breach

The individuals whose data has been lost should be contacted, with a view to advising them of any potential impact of the data loss. In the event of a serious loss of data it may be necessary to inform the ICO of the breach (e.g. loss of a large number of records).

4. Evaluation and Response

The cause of the breach must be investigated and measures put in place to prevent the breach from recurring.

Safe Use of Images

1. Consent of Adults who Work at the Academy

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Should a member of staff not wish to have their photograph used on the school website they can request its removal by the IT Services team.

2. 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 BFET 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). Consent has to be

given by both parents in order for it to be deemed valid. This consent is considered valid after the child has left the school unless school is informed otherwise.
Students' full names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published.
Where students 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. Storage of Images

- Images / films of children are stored on the school's network.
- CCTV is used for security purposes.
- Rights of access to this material are restricted to the staff and students within the confines of the school network, or via secure Remote Desktop connections.
- Images and videos of students recorded or stored on personal 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).

4. Webcams

- Webcams in school are only ever used for specific learning purposes, e.g. monitoring hens' eggs or video conferencing.
- Misuse of the webcam by any member of the community will result in sanctions.
- Consent for publication of images is assumed to extend to use of webcams.

5. Video Conferencing and Online Meetings

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of BFET.
- All students are supervised by a member of staff when video conferencing with end-points beyond BFET.
- Approval from the eSafety Coordinator is sought prior to all video conferences with end-points beyond BFET.
- The Academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the consent of the parents/carers of those taking part.

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.

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

An example letter to send to parents to notify of an Academy's intention to use biometric data in this way is included as an appendix to this policy.

Access to Records

1. Students

Students, (or their parents or carers) have the right to access the educational records (as defined in Schedule 11 of the Data Protection Act 1998) we hold about them. In order to access the records, a request needs to be made in writing, whereupon we will respond to the request within 15 school days. Records may be inspected free of change but a reasonable fee may be incurred if duplicates are requested. We may request proof of the requester's identity and may refuse access to the following:

- Information which, if disclosed, is likely to cause serious harm to the physical or mental health of the student, or someone else.
- Information as to whether the student is or has been subject to or may be at risk of child abuse, where the disclosure would not be in the best interests of the student;
- Records relating to safeguarding issues.
- References supplied to potential employers or anybody concerned with student admissions to another school, university or other institution of higher or further education or training.
- Information supplied by the school in a report to any juvenile court, where the rules of that court require the information be withheld.
- Information concerning the student which also constitutes personal information about another individual who has not consented to the disclosure of the information (unless the other individual's name or identifying particulars may easily be redacted).
- Information recorded by the student during an examination.
- Requests which have already been dealt with.

2. Staff

Staff (and former employees) also have the right to access their own personal data (as defined in Schedule 11 of the Data Protection Act 1998) we hold about them. In order to access the records, a request needs to be made in writing, whereupon we will respond to the request within 40 days. Records may be inspected free of change but a reasonable fee may be incurred if duplicates are requested. We may request proof of the requester's identity (for former employees) and may refuse access to the following:

- Information which, if disclosed, is likely to cause serious harm to the physical or mental health of the individual, or someone else.
- Information concerning the employee which also constitutes personal information about another individual who has not consented to the disclosure of the information (unless the other individual's name or identifying particulars may easily be redacted).
- References supplied to potential employers or as part of internal recruitment.
- Requests which would require disproportionate effort to supply (although we will always try and work with the subject in order to establish an equitable solution).

ICT Equipment including Portable and Mobile Equipment and Removable Media

This section should be read in conjunction with the equivalent section in the eSafety policy.

1. Academy owned ICT equipment

- It is imperative that you save your data on a frequent basis to the academy's network drive or approved cloud storage. You are responsible for the backup and restoration of any of your data that is not held on the academy's network drive or cloud storage. **No personally identifiable or sensitive data should be stored on your own equipment**.
- The safest way to ensure the safety of your data, and the security of sensitive data, is to use the Remote Desktop system provided by the academy, or approved cloud storage which meets appropriate data protection requirements.
- Personal or sensitive data must not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.

2. Portable and Mobile ICT Equipment

This section covers such items as laptops, mobile phones, tablets and removable data storage devices.

- Staff must ensure that all academy data is stored on the academy's network or approved cloud storage.
- **No personally identifiable or sensitive data may be stored on any unencrypted media.**
- Equipment must be kept physically secure in accordance with this policy. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- Use Remote Desktop to access the academy's systems where available.

3. Systems Access

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Any information held on academy systems, hardware or used in relation to academy business may be subject to The Freedom of Information Act.
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1988.

4. Telephone Services

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.
- Be aware of Data Protection legislation when engaged in telephone conversations – do not divulge personal or sensitive information. See the Data Protection policy for further guidance.

Further Information/Current legislation

Acts Relating to Monitoring of Staff e-Mail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Protection of Freedoms Act 2012

(Particularly covering the use of biometric data – see advice below)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268649/biometrics_advice_revised_12_12_2012.pdf

Local Addenda

Agreed local variations to the policy – due to technical implementation or local policy – should be documented here.

In addition, the names and locations of staff and appropriate documentation should be entered into the tables below:

Role	Staff member
SIRO	Sue Warner

Documentation	Location
Data protection policy	eSafety Staff shared area and website
eSafety log	eSafety Staff shared area

Privacy Notice - Data Protection Act 1998 – for Staff *(needs adapting locally)*

(Academy Name) are the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector.
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up.
- Informing the development of recruitment and retention policies.
- Allowing better financial modeling and planning.
- Enabling ethnicity and disability monitoring.
- Supporting the work of the School Teachers' Review Body.

Staff photographs are used for identification purposes but are not published without consent.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as photographs, ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school, Trust or Local Authority (LA) without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:

- the Local Authority (LA)
- the Department for Education (DfE)

It may also be necessary for us to share information with Bright Futures Educational Trust.

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- http://www.trafford.gov.uk/about-your-council/data-protection/privacy-notices/privacy-notices-school-workforce.aspx
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites, please contact the LA or DfE as follows:

	Local Authority	**Department for Education**
Phone	Local LA Phone No	0370 000 2288
Email	Local LA Email	info@education.gsi.gov.uk https://www.gov.uk/government/organisation/department-for-education
Post	Local LA Address	Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT

Privacy Notice - Data Protection Act 1998 – for Students *(needs adapting locally)*

(Academy Name) are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data to:

- Support your learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well we are doing.

(Academy Parent Portal Name) is provided to enable you and your parents/carers to access information about your attendance and progress in addition to submitting requests to change the information we hold about you. Access to this system is restricted by usernames and passwords which have been given to your parents/carers.

We take photographs of students for identification purposes but also for publicity. If your parents / carers do not want your photograph or video recordings to be published online or in the media they have the right to opt out by contacting the school or registering their preference on SLG.

Examination scripts, coursework items or recordings (e.g. drama performances or oral assessments) containing personal information such as name and candidate number will be shared with the relevant examination boards. The information may be transmitted electronically, or via the postal service in electronic or paper form.

From time to time it may be necessary to share information about you with external agencies or organisations – e.g. for school trips.

CCTV is used around the school for crime prevention purposes. Recordings may be made of lessons for staff appraisal or reflection.

Information about you that we hold includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs you may have and relevant medical information. If you are enrolling for post 14 qualifications the Learning Records Service will give us your unique learner number (ULN) and may also give us details about your learning or qualifications.

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide the names and addresses of you and your parent(s), and any further information relevant to the support services' role. We may also share data with post 16 providers to secure appropriate support on entry to post 16 provision.

However, parent/carer(s) can ask that no information beyond names, addresses and your date of birth be passed to the support service. This right transfers to you on your 16th birthday. Please tell ***(Staff Person Responsible)*** if you wish to opt out of this arrangement. For more information about young people's services, please go to the National Careers Service page at https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx

We will not give information about you to anyone without your consent unless the law and our policies allow us to do so.

Information Asset Register – *(To be adopted for each school)*

Bright Futures
EDUCATIONAL TRUST

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk
SIMS MIS	Sue Warner, Stuart Cairns	Restricted	Low	Medium	Access via passwords with complexity requirements. Data stored on password protected server in locked room – backups locked in switch cabinet. VPN access for communication with SLG hosted service.
Network file areas	Sue Warner, Stuart Cairns	All classification	Low	Medium	Access via passwords with complexity requirements. Data stored on password protected server in locked room – backups locked in switch cabinet. Secure Remote Desktop access for access to Protect/Restricted documents. Shadow copies for protection against accidental deletion. Protected folders marked with security owner text file for restricting write (or even read) access.
SLG	N/A	Restricted	Low	Low	Communication with school MIS via encrypted VPN. All users require passwords with minimum complexity limits.
Teacher's Planners	Individual staff	Protect / Restricted	Low	Low	Kept out of sight when not in use.
Medical information booklets	Individual staff	Restricted	Low	Medium	Must be kept out of sight when not in use – inside planner, etc
Trip Lists	Trip organisers	Protect / Restricted	Low	Low	Lists to be produced immediately prior to trip departure – issued to trip leaders in trip folders – kept with leaders at all times – shredded by trip organiser upon return
Analysis spreadsheets	Individual HODs	Protect	Low	Low	Stored in Staff / Teacher's area of network – only accessed externally by secure Remote Desktop.
School Website	Paul Morgan	Unclassified	Low	Low	Access to CMS backend by https and strong passwords.
CCTV Security Cameras	Paul Walsh	Protect	Low	Low	Accessed only via onsite hardware in locked offices
Child Protection Register	Jill Cinan	Restricted	Low	Low	Information stored in locked cabinet in locked office. Limited access.
SEND list	N/A All students SEND	Restricted	Low	Low	
Staff records	Yvonne Reil	Restricted	Low	Low	Locked in main office
Financial records	Audrey Whelan	Protect	Low	Low	Paper records locked in finance office – FMS data stored on password protected server in locked room – backups locked in switch cabinet.

APPENDIX 2

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk
Staff payroll records	Yvonne Reil/ Audrey Whelan	Restricted	Low	Low	Paper records locked in finance office – FMS data stored on password protected server in locked room – backups locked in switch cabinet.
ParentPay	**N/A**	Protect	Low	Low	Online service via HTTPS connection
ParentMail	**N/A**	Protect	Low	Low	Online service via HTTPS connection
Exam results	Nicola Hammond, Robert Barlow	Protect	Medium	Low	Data stored on MIS systems – both SIMS and (historical data) CMIS – likelihood classed as medium until CMIS historical data has been archived (into simple Excel list?)
School fund lists	Audrey Whelan	Restricted	Low	Low	Copies of standing order forms remain in locked drawer. Paper copies kept locked in finance office, transported in locked boot where necessary.
Photocopier numbers	Stuart Cairns	Protect	Low	Low	Locked in cabinet in Reprographics room, backup of list stored on network
Form lists	Heads of Departments	Unclassified	Low	Low	Accessible to all staff in the Reprographics room, but contain no data other than student names.
Alarm access codes	Paul Walsh				
Digital door codes	Paul Walsh				
Training lists	Julie Barnett, Maree Jordan				