Bright Futures

EDUCATIONAL TRUST

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

eSafety Policy

Including guidance on:

Protecting and educating staff and students in the safe use of technology, implementing appropriate mechanisms to intervene and support any incidents and, where appropriate, enforcing relevant legislation and upholding best practice.

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

Date of Policy Approval:	2017, reviewed April 2019
Owner of Policy:	**Chief Operating Officer**
Authorised By:	**Executive team**
Policy Review Date:	**April 2021**
Distribution:	**All Trust Staff** **All Members/Trustees/ Governors** **Consultants working on behalf of the Trust** **Trust/Academy Websites**

E-SAFETY POLICY

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;
- Three of our commitments: **Effective Communication, Professional Learning** and **Strong Governance and Accountability.**

What is the Policy for?

Digital technologies in the 21st Century are seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. We must also ensure compliance with data protection laws when we collect, process and store personal information about individuals.

Whilst exciting and beneficial both in and out of the context of education, much digital material, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that some have a minimum age, usually 13 years.

Digital technologies cover a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of digital technologies within our society as a whole. Currently the resources children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, vlogs and Wikis
- Podcasting
- Video Broadcasting/Streaming
- Music Downloading/Streaming
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Tablets and other mobile devices with web functionality

As BFET academies, we understand the responsibility to educate our students on eSafety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Academies 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 Academies. The Trust has technical and organisational measures in place to keep this information safe which all users must adhere to.

This policy is inclusive of both wifi and 4G connectivity, technologies provided by the school (such as PCs, laptops, smartphones, tablets, webcams, whiteboards, voting systems, digital video equipment, etc) and hardware owned by students and staff, but brought onto school premises (such as laptops, mobile phones, smartphones and portable media players, etc "Bring Your Own Device" (BYOD)).
This policy is based on the guidance document developed by Hertfordshire Grid for Learning, which can be found here: http://www.thegrid.org.uk/eservices/safety/policies.shtml

Other material from additional sources is credited where relevant.

Who is the Policy for?

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 are made aware of the risks and threats and how to minimise them.

Policy Standards

A few definitions:

Term	Brief definition
BYOD	"Bring Your Own Device" – general term covering the use of non-Academy devices on the Academy network.
Data	Information in the form of text, numbers, scores, images, video, etc (pretty much anything which may be stored electronically)
Personal Data	any information relating to an identified or identifiable living individual also known in law as a 'data subject'
Encryption	Turning data (e.g. text, images, etc) into "code" which cannot be turned back into the original data without the use of a "key" (usually a password of some kind)
IAO	Information Asset Owner (see Data Protection Policy)
LADO	Local Authority Designated Officer
Malware	Generic term for any software intended to do something undesirable. This includes viruses (which spread from machine to machine) and spyware (which surreptitiously

Term	Brief definition
	collects information).
Personally identifiable data	Data relating to a (living) individual who can be identified from those data (or other information likely to be available) and includes opinions or what is intended for them (e.g. report comments or assessment scores). Note this includes any class list containing any kind of data. For further details see this quick reference guide produced by the Information Commissioner's Office. Note that any reference to the religion, or racial or ethnic origin of the individual is subject to stricter controls.
Portable device	Any piece of hardware which is intended to be removed from the school site. Includes laptops, mobile phones, tablets and memory sticks.
Sensitive data	Any information which could be harmful if it were to find its way into the public domain. This includes (but is not limited to): personally identifiable data, confidential information about individuals, the school, or BFET, commercially confidential information such as financial details, etc.
SIRO	Senior Information Risk Officer (see Data Protection Policy)

Specific Standards

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by an Academy at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, files, e-mails, instant messaging, computer or internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Academy business related information, to confirm or investigate compliance with Academy policies, standards and procedures, to ensure the effective operation of Academy digital technologies. It may also be for quality control or training purposes, to comply with a Subject Access Request under the General Data Protection Regulation, safeguarding of pupils and students or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation and the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using or accessing school resources may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. When using Trust IT systems all data processed is under our control and is subject to all applicable laws, including data protection law.

Breaches and Incident Reporting

A breach or suspected breach of policy by a BFET employee, contractor or student may result in the temporary or permanent withdrawal of Academy digital technology hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the Academy's Disciplinary Procedure or, where appropriate, the BFET Disciplinary Procedures or Probationary Service Policy.
For pupils any breaches will be handled according to the school's respective behaviour policy.

Policy breaches may also lead to criminal or civil proceedings.
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Academy's eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including passwords), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the eSafety Coordinator.

Please refer to the section below on Incident Reporting, eSafety Incident Log & Infringements.

Acceptable Use Policies **(AUP)**

Model AUPs for students and staff are included as appendices at the end of this document.

Malware

All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB memory stick) must be checked for any viruses using academy provided anti-virus software before using them.

Never interfere with any anti-virus software installed on school ICT equipment that you use. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through IT Services.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your IT Services team immediately. IT Services will advise you what actions to take and be responsible for advising others that need to know.

Never open an email attachment unless you are sure of its origin – even if it looks plausible. **If in doubt: delete**. Genuine emails can always be resent.

Signs of possible malware infection include:

- Browser pop-ups.
- Redirected home page or search pages (i.e. not what you are used to).
- Sudden, abnormally poor performance (although this may be caused by a number of factors).
- Alarming warnings from software you haven't come across before.

If you are in doubt, speak to a colleague, your manager or member of your IT Services team.

In the event of a suspected virus or other malware infection, the following procedure should be followed:

- Immediately notify IT Services of the suspected incident.
- Switch off the equipment and, where practical, warn other users of the possible issue.
- Remove any writable, removable media from the machine and pass this to IT Services.

IT Services will then:

- Isolate the machine and removable media from the network.
- Run an updated, stand-alone virus removal tool on the suspected machine and media.
- Verify the state of virus protection on the main servers.

- Check the state of the infection on the suspect hardware and either:
  - Return it to the network / user if virus removal has been successful.
  - Re-install / re-image / re-format the device if the removal cannot be confirmed.

Email

The use of e-mail within most academies is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private – Freedom of Information requests and subject access requests may include email trails, for instance. Educationally, e-mail can offer significant benefits, for instance direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and intended recipient. BFET expects all users to ensure that e-mail communications are appropriate and not used in any way to cause intentional damage or distress to individuals.
See the separate Data Protection policy for further details and guidance.

Managing email

The academy may give all staff (and students) their own e-mail account to use for all academy business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The academy email account should be the account that is used for all academy or BFET business.

- **Under no circumstances should staff contact students, parents/carers or conduct any academy or BFET business using personal e-mail addresses. Staff should never use students' personal email addresses under any circumstances.**
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on headed paper.
- All student e-mail users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the eSafety Coordinator if they receive an offensive e-mail.
- Students are introduced to e-mail as part of the ICT or Computing Scheme of Work.
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending emails

- **Email is an insecure medium. It should not be used for sending personally identifiable or sensitive information (i.e. anything classified as "Protect" or "Restricted" in accordance with the Data Protection policy).** If you need to send such information within your academy, please store the information on the network and simply indicate to the recipient where the information may be found. If you need to send such information to another email domain, please check with the relevant IAO and contact IT Services for advice. Always check the recipient prior to sending.
- Use your own academy e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location on a shared drive / online folder rather than sending attachments.
- Academy e-mail is not for personal use – and will no longer be available once you leave the academy's employment.

Receiving emails

- Check your e-mail regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments or click on links from an untrusted source.
- **If in doubt: delete.**

eSafety

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the Academy, the Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Academy will nominate a named eSafety Coordinator who will be designated this role. All members of the Academy community must be made aware of who holds this post. It is the role of the eSafety Co-ordinator to keep abreast of current issues and guidance through organisations such as the local authority, BFET, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Principal/eSafety Co-ordinator and all Governors have an understanding of the issues and strategies at the Academy in relation to local and national guidelines and advice.
This policy, supported by the academy's acceptable use agreements for staff, governors, trustees, members, visitors and students, is to protect the interests and safety of the whole community.

eSafety in the Curriculum

Digital technologies and online resources are increasingly used across the curriculum. It is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within the curriculum and academies must continually look for new opportunities to promote eSafety.

- The academy must have a framework for teaching internet skills as part of the curriculum – for instance CEOP resources (covering Internet safety, cyber bullying and related issues) may be embedded in the curriculum and delivered to all year groups.
- Educating students on the dangers of technologies that may be encountered outside the academy may be done informally when opportunities arise and as part of the eSafety curriculum.
- Students are taught about copyright and respecting other people's information, safe use of images, taking and recording of pictures and videos, etc. through discussion, modelling and activities.
- Students must be aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button (on all BFET websites), in addition to local solutions such as the "Sharp System."
- Students are taught to evaluate materials critically and learn good searching skills through cross curricular teacher models, discussions and via the specific ICT curriculum.

eSafety Skills Development for Staff

- Staff must receive regular information and training on eSafety issues in the form of INSET training and updates, together with this e-safety policy.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the Academy eSafety Messages

- Endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy should be introduced to the students at the start of each school year.

Incident Reporting, eSafety Incident Log and Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the academy's eSafety Co-ordinator. Additionally,

all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of digital technologies and all other policy non-compliance must also be reported.

eSafety Incident Log

Any incidents should be recorded by the eSafety Coordinator in the eSafety log, stored securely in a documented location on the academy's network – the layout of which is presented below:

Date & Time	Name of student or staff member	Gender	Room and computer or device identifier	Details of incident (including evidence)	Actions and reasons

Misuse and infringements

Complaints

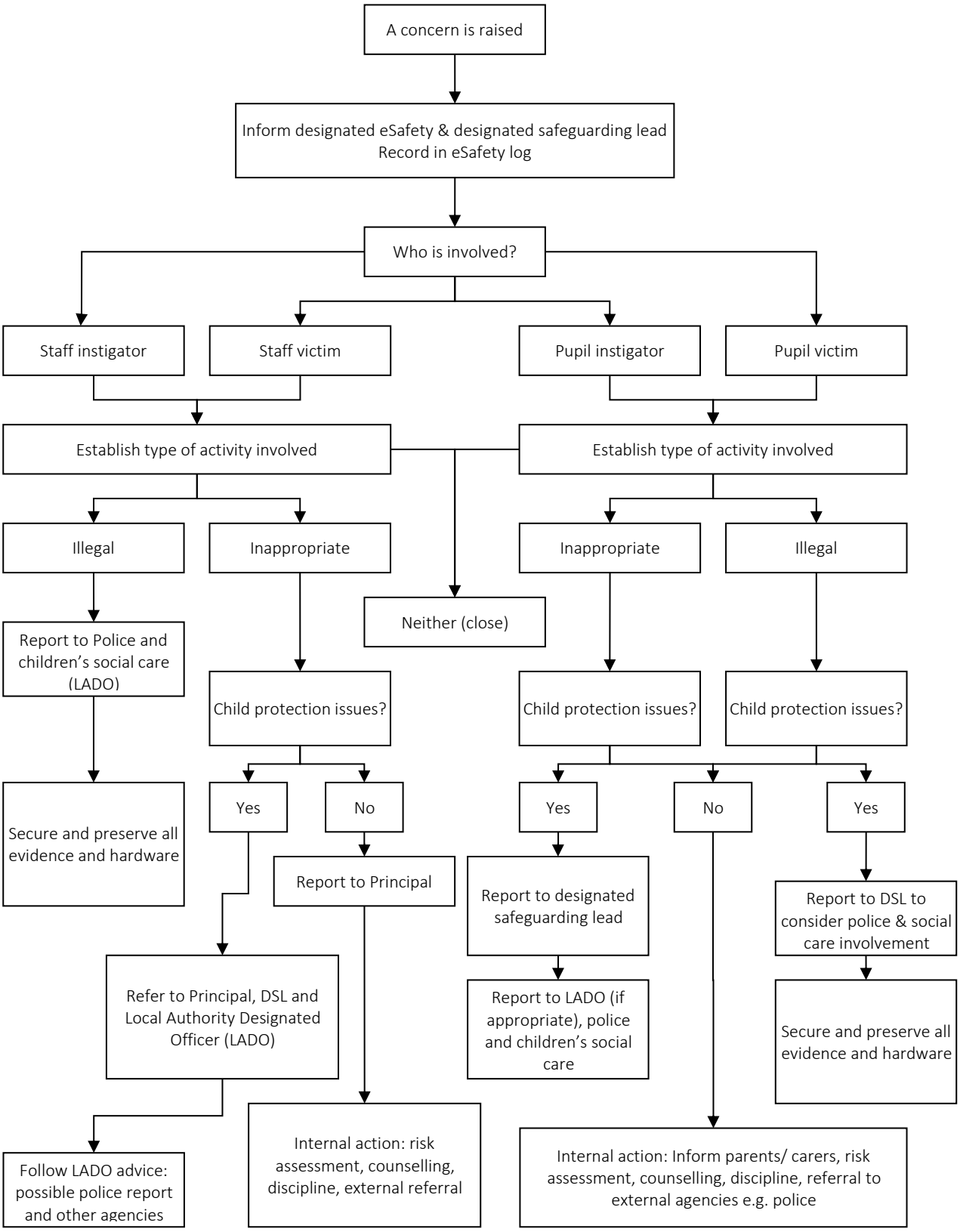
Complaints and/or issues relating to eSafety should be made to the eSafety co-ordinator or Principal. In the case of matters that have a safeguarding dimension, staff should follow their safeguarding reporting protocols, reporting to the Designated Safeguarding Lead. Incidents should be logged and the flowchart (see below) should be followed. Some incidents may also require reporting and input from the Data Protection Officer ("DPO").

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety Co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being referred to the Designated Safeguarding Lead, logged by the eSafety Co-ordinator and, depending on the seriousness of the offence, formal investigation. Immediate suspension from duties may be imposed, possibly leading to dismissal and involvement of the police for very serious offences (see below).
- Users are made aware of sanctions relating to the misuse or misconduct in the staff handbook.

Flowchart for managing an eSafety incident.

This is an example and each case may be different.



Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The academy will provide students and staff with supervised access to Internet resources (where reasonable) through the academy's fixed and mobile internet connectivity.
- Staff must preview any recommended sites or online systems before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute academy software or software from other sources.
- All users must observe copyright of materials from electronic resources – information made available online cannot be assumed copyright free.

Internet use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Be careful with work related information when using social media, in particular using student's names.
- On-line gambling or gaming is not permitted.

Infrastructure

Details of the local infrastructure, the filtering and safeguarding measures in place are detailed in the local addenda section.

Prevent duty

Guidance on the Counter-Terrorism and Security Act 2015 – to have due regard to the need to prevent people from being drawn into terrorism (a.k.a. "Prevent") – explicitly states that:
'Specified authorities will be expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.'
While this duty does not confer new functions on any specified authority (i.e. BFET or the individual academies), '*the term "due regard" as used in the Act means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions'*. Hence there is an expectation to pay specific attention to the filtering of sites which could be seen as likely to draw young people into terrorism, or to extremist ideologies.
Academies must therefore ensure that filtering and monitoring systems are able to trap sites and material likely to be covered by the Act. Where a student is found to be accessing such material without legitimate purpose (e.g. as part of a Citizenship assignment), it should be treated as a safeguarding issue. Further guidance is available in the Trust's Child Protection and Safeguarding: Policy, Procedures & Guidance here.

Social Media (and other "web 2.0" technology)

Online technology, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities.

However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

1. Students:

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report anything which causes them concern (e.g. incidents of bullying, inappropriate requests for contact) to the school or a trusted adult
- In extreme cases, where a student feels threatened or at risk, the student should immediately contact the NCA's CEOP Command via the link () at the top left of all BFET websites
- Students must not use public social media for school business without the knowledge of the eSafety Coordinator. Students wishing to have a blog created for an approved school group, society, team or event may contact IT Services who will be happy to oblige or advise further.

2. Staff:

- Staff may only create blogs, wikis or other online systems in order to communicate with students using systems approved by the eSafety Coordinator. We do not permit any use of Facebook or other social media sites to engage with students for social purposes but may allow access to such sites by individual approval and agreement with the eSafety Coordinator (with controls introduced to minimise opportunity for abuse) for educational purposes (within the terms set out by the site which may prohibit such use).
- If you need to disclose your professional role in any capacity when using social media be careful when you do and be mindful of what you share.
- The eSafety Coordinator must be informed of any blogs created or endorsed by members of staff for use with students. These blogs must either require passwords or moderation before posts can be added.
- Staff must ensure that all posts made on social networking sites, whether inside or outside of the academy, reflect the high professional standards expected by BFET.
- Staff must not use social networking sites as a forum to make derogatory comments which could bring the academy into disrepute, including comments about members of the academy community or BFET.
- Staff are expected to demonstrate honesty and integrity and uphold public trust and confidence in respect of anything placed on social networking websites.

- Staff must ensure that any content shared on any social networking website, e.g. Facebook, Instagram etc at any time, would be deemed as appropriate. Staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Staff must ensure appropriate language is used at all times for any comments placed on social networking sites.
- Staff must ensure that any communication and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation including data protection laws (for further guidance speak to the Data Protection Officer).
- Friend requests (or equivalent) from students must be declined and reported to the member of staffs' line manager
- Staff must not establish contact with students through their personal social networking sites, or any other means of electronic communication (including personal email or telephone). All contact with students must be directly concerned with the students' education.
- We advise that staff refrain from contacting former students via personal email or social media. Any contact should be in accordance with our data privacy policies and other related staff policies.
- Staff should exercise caution in the use of social media where their "digital social circle" (i.e. Friends, Followers, etc) may include other members of the academy community, particularly parents. Be aware that this may lead to indirect communication with students – it may be prudent to "unfriend" such individuals or at least inform a line manager via email of any such connections.
- Staff must not publish photographs, videos or any other types of image of students or their families on personal social networking accounts, or school accounts where permission for publication of images has not been granted.

Parental/Carer Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to digital technologies and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on academy website)
- The academy disseminates information to parents relating to eSafety where appropriate in the form of:
    - Information evenings
    - Website postings
    - Email
    - Twitter/Facebook
    - Newsletter items

ICT Equipment including Portable and Mobile Equipment and Removable Media

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

1. Academy owned ICT equipment

- As a user of IT, you are responsible for any activity undertaken on the academy's ICT equipment provided to you
- The academy logs IT equipment issued to staff and record serial numbers as part of the academy's asset register
- 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.
- A time locking screensaver is applied to all machines. Please lock your machine when you move away from it – even momentarily.
- Privately owned ICT equipment may only be connected to the Wi-Fi network – contact your IT Services team for further guidance.
- On termination of employment, resignation or transfer, return all IT equipment to your Manager. You must also notify IT Services so that accounts can be disabled.
- All IT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - Liaising with IT Services to ensure compatibility and to benefit from the Trust's purchasing schemes
    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed
    - All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

2. Portable and mobile ICT equipment

This section covers such items as laptops, mobile phones, tablets and removable data storage devices. Please refer to the data protection policy document when considering storing or transferring personal or sensitive data.

- All activities carried out on academy systems and hardware will be monitored in accordance with the general policy
- Ensure portable and mobile IT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the IT Services team, fully licensed and only carried out by IT Services.
- In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.
- All removable storage devices used to transport work related files must be encrypted.
- All removable storage devices connected to Academy or Trust owned devices must be encrypted.

3. Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and

misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in an academy is allowed. See the Data Protection Policy and local addenda for further details.

4. Bring Your Own Device (BYOD)

- The academy allows staff to bring in personal mobile phones and devices for their own use.
- Students may be allowed to bring personal mobile devices/phones to the academy but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent unless specific teacher permission has been given.
- In these circumstances the data contained on these devices does not come within the control of the Trust as a Controller under data protection law.
- This technology may be used, however for educational purposes, as mutually agreed with the eSafety Coordinator. The device user, in this instance, must always ask the prior permission of the bill payer.
- It is the responsibility of the device owner to ensure the device is suitably charged and in good working order.
- Where devices are required for lessons, the academy will make devices available for loan as an alternative to BYOD.
- The academy or Trust is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate communication between any members of the academy community is not allowed.
- Permission must be sought before any video, image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Devices used in lessons must be connected to the academy's own filtered Wi-Fi in such a way that the user of the device may be identified so that appropriate filtering policy may be applied and monitored. The academy cannot be responsible for web sites or services accessed through other forms of mobile internet access (e.g. 3/4G connections).
- Mobile internet sharing / hotspots should be disabled as they can interfere with the academy's own Wi-Fi connection.

5. Academy Provided Mobile Devices (including phones)

- Mobile Device Management software should be installed onto all academy owned portable devices for management and monitoring.
- The sending of inappropriate communication between any members of the academy community is not allowed.
- Permission must be sought before any video, image or sound recordings are made on the devices of any member of the academy community.
- Where the academy provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- The personal data contained on these devices does come under the control of the Trust as Controller and users are obliged to handle this data in accordance with the Data Protection policy.

Systems Access

- You are responsible for all activity on academy systems carried out under any access/account rights assigned to you, whether accessed via academy IT equipment or your own hardware.
- All access to IT systems and the internet must be via approved systems which provide appropriate management, filtering and security – users (staff or students) must not attempt to circumvent these measures for any reason. If in doubt, contact your local IT Services.
- Do not allow any unauthorised person to use academy IT facilities and services that have been provided to you.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from academy ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the academy, BFET or LA into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the academy's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Equality Act 2010).

Landline telephone services

- You may make or receive personal telephone calls provided:
  - They are infrequent, kept as brief as possible and do not cause annoyance to others.
  - They are not for profit or to premium rate services.
  - They conform to this and other relevant BFET and academy policies.
- Academy telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
- Ensure that your incoming telephone calls can be handled at all times by leaving appropriate voicemail messages or diverting to a colleague.

Mobile phones & other portable devices

- You are responsible for the security of your academy mobile phone or device.
- Report the loss or theft of any academy mobile phone or device immediately – the academy remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your academy mobile phone prior to using it.
- Academy SIM cards must only be used in academy provided mobile phones.
- Academy mobile phones may be barred from calling premium rate numbers and any numbers outside of the UK.
- You must not send text messages to premium rate services
- You must reimburse the academy for the cost of any personal use of your academy mobile phone. This includes call charges incurred for incoming calls whilst abroad.

Further Information/Current legislation

Acts relating to monitoring of staff email and activity

GDPR and Data Protection Act 2018

The above legislation requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The legislation 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

Other Acts and guidance relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

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.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Keeping Children Safe in Education (2018)

Acts Relating to the Protection of Personal Data

General Data Protection Regulation

https://gdpr-info.eu/

Data Protection Act 2018

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

The Counter-Terrorism and Security Act 2015:

http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted

Specific guidance for schools can be found in sections 57-76 of the following document:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

Local addenda

Agreed local variations to the policy – due to technical implementation – 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
eSafety Coordinator	
eSafety link governor	
IT Services team	

Documentation	Location
Data protection policy	
eSafety log	

Local infrastructure - *this will need adapting locally*

- (Name of Local Authority) has a monitoring solution where web-based activity is monitored and recorded.
- Fixed (Name of Academy) internet access is controlled through the (Name of Provider).
- BYOD internet access in controlled through and onsite web filter – note that the filtering rules of these two systems may not precisely coincide.
- Staff and students are aware that school based computer and internet activity can be monitored and explored further if required.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the IT Services team's, to install or maintain virus protection on personal systems. Free malware protection for Microsoft Windows (version 7 onwards) may be obtained from www.microsoft.com by searching for "Security Essentials".
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from network manager.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via IT Services helpdesk.

- If you require a site that is normally blocked to students open in an IT suite or on mobile internet devices this must be raised on the IT Services helpdesk in a timely manner (i.e. with at least 24 hours' notice).

APPENDIX 1 (Only Required if Applicable to Academy and can be Adapted)

Acceptable Use Agreement: Students

- I will only use ICT systems in the academy, including the internet, e-mail, digital video, mobile technologies, etc. for academy purposes.
- I will not download or install software on academy equipment without approval by the IT Services team.
- I will only log on to the academy network or other areas or platforms with my own user name and password.
- I will follow the academy's ICT security system, password recommendations and not reveal my passwords to anyone and change them as required.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for academy purposes in line with academy policy and not be distributed outside the school network without the permission of the eSafety Coordinator. **I will not take recordings, images or videos of other members of the school community (including other students and teachers) without their knowledge or consent.**
- I will ensure that my online activity, both in school and outside school, will not cause my academy, the staff, students or others distress or bring into disrepute. This includes the use of social media sites (including Facebook), blogs and microblogging sites (such as Twitter) and media sharing sites and apps (such as Snapchat).
- I will support the academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the academy community both inside and outside of the academy.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, academy sanctions will be applied and my parent/ carer may be contacted.
- If I do not have access to an internet connection or other required technology to complete a piece of work I will do the work on the computers at the academy or print the work at the academy and complete on paper.
- I will comply with the Data Protection Policy and ensure that I adhere to any policies and procedures issued by BFET for the use of personal data.

✂ ----------✂---------- ✂---------- ✂---------- ✂---------- ✂

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT. Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their form teacher.

Please return the bottom section of this form to school for filing.

Student and Parent/carer signature

We have discussed this document and .....(student name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at AGGS. I am aware that my daughter may be required to access approved online resources or social media as part of her homework but that offline alternatives will be made available where necessary.

Parent/Carer Signature .....

APPENDIX 1 (Only Required if Applicable to Academy and can be Adapted)

Acceptable Use Policy: Sixth Form Students

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school equipment.
- I will only log on to the school network or other areas or platforms with my own user name and password.
- I will follow the schools ICT security system, password recommendations and not reveal my passwords to anyone and change them as required.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the eSafety Coordinator. **I will not take recordings, images or videos of other members of the school community (including other students and teachers) without their knowledge or consent**.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute. This includes the use of social media sites (including Facebook), blogs and microblogging sites (such as Twitter) and media sharing sites and apps (such as Snapchat).
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community both inside and outside school.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.
- If I do not have access to an internet connection or other required technology to complete a piece of work I will do the work on the computers at school or print the work at school and complete on paper.
- I will comply with the Data Protection Policy and ensure that I adhere to any policies and procedures issued by BFET for the use of personal data.

✂ ---------- ✂ ---------- ✂ ---------- ✂ ---------- ✂ ---------- ✂

Dear Student

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their form teacher.

Please return the bottom section of this form to school for filing.

Student signature

I have read this document and I, ...(student name), agree to follow the eSafety rules and to support the safe and responsible use of ICT at (Academy Name). I am aware that I may be required to access approved online resources or social media as part of homework but that offline alternatives will be made available where necessary.

Student Signature…… Date ……

Form ……. Name (Block Capitals) …….

APPENDIX 2 (To be Adapted if Appropriate)

Acceptable Use Agreement: Staff, Governors Trustees, Members and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. This document is intended as guidance and recommendations for the protection of all members of the school community. Any concerns or clarification should be discussed the academy eSafety Coordinator.

- I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed reasonable by the Principal or Governor responsible for eSafety.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not use my school email account for personal use (e.g. online shopping sites, mailing lists
- I will not forward confidential school emails to non-school accounts, or access school email by any insecure method (usual web access *is* considered secure). I will report the loss of any mobile device with access to school email to IT Services immediately so it may be wiped remotely.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- If I use social media I am aware of the potential risks and the recommendations contained within the eSafety and Data Protection policies – and will act in accordance with the Teachers' Standards where appropriate.
- I will use the approved, secure e-mail system(s) for any school business.
- I have read and understood the school's Data Protection Policy.
- If I intend to use my own devices for school use (including email) I will comply with the BYOD section of the Data Protection Policy.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school or accessed remotely.
- I will not store, transfer or transmit by email attachment or other insecure method any personally identifiable information (including class lists). **I understand that this prohibits the use of unencrypted memory sticks or other portable media for transferring data about specific, identifiable (i.e. named) students, or storing any such data on computers outside of school.**
- I will not install any hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory unless reasonably part of lesson content.
- I will refer to the Storage of Images section of the Data Protection Policy for the taking and processing of images of students.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or eSafety Coordinator.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute, in accordance with the Teaching (or other professional) Standards where appropriate.
- I will support and promote the school's e-Safety and Data Protection policies and help students to be safe and responsible in their use of ICT and related technologies.
- I will comply with the Data Protection Policy and ensure that I adhere to any policies and procedures issued by BFET for the use of personal data.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the Academy.

Signature …….. Date …….

Full Name …….. (BLOCK CAPITALS)