THE EDUCATION VILLAGE ACADEMY TRUST

E-Safety Policy

EVAT Version Control Document

Version:	Date:	Policy Owner:	Amendments made by:	Details of amendments made:	Reviewed by:	Approved by:
V1.0	16.3.16	Richard Gartland		Final version	ELT	ELT
V1.1	17.3.16	Richard Gartland	Richard Gartland	Addition of note regarding Tapestry.	Cathy Knights	N/A
V2.0	06.09.17	Jonathan Lumb	W Turpin	Reformatted		
V2.1	22.03.18	Jonathan Lumb	Jonathan Lumb	Addition of information on removable data storage media and passwords	Alana Mackenzie	ELT March 2018
V2.2	19.11.18	Jonathan Lumb	Alana Mackenzie	KCSIE new requirements P29	Cathy Knights	N/A
V2.3	22.11.18	Jonathan Lumb	Wendy Turpin	Para relating to display of images on apps/newsletters & para relating to Governance.	Alana Mackenzie	
V2.4	20.12.18	Jonathan Lumb	Wendy Turpin	Clarity regarding pupils names on the internet being only first name and initial	Jonathan Lumb	

Monitoring and review

This policy is reviewed every **two years** by the Policy Owner: **J Lumb**

The scheduled review date for this policy is **March 2020**.

The Education Village Academy Trust
Where learning has no limits

Where learning has no limits

At The Education Village Academy Trust, all children, young people and adults are valued both as individuals and as part of the wider Trust community. We aim to provide a safe, happy and caring environment within which everyone can thrive.

Core values

Our Trust's activities are informed by our core values, which mean that we:

1. recognise the ***worth*** of each ***individual*** by valuing the personal qualities they demonstrate in their learning, living and working
2. recognise the ***experiences*** of children and young people by valuing the ***talents*** and ***skills*** they bring into their schooling, and we commit to ensuring that schooling enhances these talents and skills
3. embrace ***difference*** and ***harmony*** by valuing ***diversity***
4. display ***integrity*** and ***authenticity*** by valuing ***openness***, ***trust***, ***fairness***, ***honesty*** and ***respect*** for all people
5. foster ***ambition, high aspirations*** and ***independent*** spirit by valuing each individual's abilities, aptitudes and desire to create, explore and grow
6. commit to ***hard work*** and ***high standards*** in provision, behaviours and outcomes
7. help, support and enable others by valuing ***relationships*** with all stakeholders, being ***emotionally intelligent***, building ***resilience*** and being ***forward-looking***
8. acknowledge the role of ***networks*** by valuing the ways in which people can live together, collaborate and make positive contributions as ***citizens***
9. acknowledge the place of school in the ***community***, including the broader ***global*** community, by valuing the essential nature of the relationship between schools and the social and economic environments in which they operate

This policy, and its associated procedures and protocols, are based on these key principles.

Contents

N.B. Where reference is made to an 'Academy' or a 'School' the intention is that the policy is universal and applies to both.

Introduction

ICT in the 21st Century is 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.

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

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, 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 internet technologies and that some have minimum age requirements (13 years in most cases).

At The Education Village Academy Trust we understand the responsibility to educate our pupils on e-Safety 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.

Schools hold personal data on learners, staff and others 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.

Everybody in the Trust community 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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the Trust (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

This policy should be read in conjunction with the following Trust policies:

- Code of Conduct for Trust employees
- Disciplinary Policy
- Protecting Children from Extremism and Radicalisation Policy
- Safeguarding and Child Protection Policy
- Staff Social Media Policy
- GDPR Data Protection Policy

Within this policy the definition of '*school*' refers to both an academy and Free School.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

The staff authorised to carry out the inspection of IT equipment are:

- Chief Executive
- Principles
- IT & Media Manager
- Senior IT Technicians

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone call records, emails, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of

school ICT; to comply with a Subject Access Request under the Data Protection Act 1998 and General Data Protection Regulation (GDPR) or to prevent or detect crime.

Breaches

A breach or suspected breach of policy by a Trust employee, contractor or pupil may result in the temporary or permanent withdrawal of Trust ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers allow the Information Commissioner's office to serve notices requiring organisations to pay up to €20m for serious breaches of the General Data Protection Regulation (GDPR).

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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 Trust's Data Protection Officer or Chief Executive in order that breaches can be reported to the Information Commissioners Office (ICO) within 72 hours. 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 Trust's Data Protection Officer or Chief Executive.

Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

Primary Pupil Acceptable Use

Agreement / e-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords including my FROG password.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own/other's details such as name, phone number or home address.
- I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school or wider community.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will not sign up to online services until I am old enough. I will observe age restrictions.

Dear Parent/Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our Trust. We expect all children to be safe and responsible when using any ICT including our FROG virtual learning environment (VLE).

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns, or would like some explanation, please contact your child's school Principal.

Please take care to ensure that appropriate systems are in place at home to protect and support your children.

✂---

Parent/ carer signature

We have discussed this document with;

……………………………………......... (child's name) and we agree to follow the e-Safety rules and to support the safe use of ICT at [insert school name].

Parent/ Carer Signature ……..………………….…………………………….

Class …………………………………. Date ………………………………

Acceptable Use Agreement: Student - Secondary

- I will only use ICT systems in school, including the internet, email, digital video and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communication with pupils, 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 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.
- I am aware that when I take images of pupils / staff, I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- 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 related 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.
- I will not sign up to online services until I am old enough to do so.

Dear Parent/ Carer

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT including our FROG virtual learning environment (VLE).

It is essential that students are aware of e-Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent/ carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with the Principal of [insert academy name].

Please return the bottom section of this form which will be kept on record at the school

✂----------

Parent/ carer signature
We have discussed this document with;

…….. [insert your child's name] and we agree to follow the e-Safety rules and to support the safe use of ICT at [insert academy name].

Parent/ Carer signature ……

Student signature……..

Tutor Group…… Date ……

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

- ICT (including data) and the related technologies such as email, our VLE, the internet and mobile devices are an expected part of our daily working life across EVAT. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Trust's Chief Executive.
- I will only use the school's email / Internet / Intranet / FROG VLE and any related technologies for professional purposes or for uses deemed acceptable by the Chair of the Board of Directors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Trust or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal social media account links to pupils.
- I will only use the approved, secure email system for any Trust business.
- I will not install any hardware or software without permission of the Chair of the Board of Directors.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with Trust policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the Trust network without the permission of the parent/ carer, member of staff or Principal.
- I will support the Trust approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community.
- I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available, on request, to a member of the Executive Leadership Team.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the Trust, my professional reputation, or that of others, into disrepute.
- I will support and promote the Trust's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use removable data storage media (e.g. USB sticks, portable hard drives) to transfer data between their place of work and home (or any other remote location).
- Only, in the most exceptional one-off circumstances, at the discretion and with the written permission of either a Principal or the Chief Executive, will I use a removable data storage media, provided by EdIT Learning Ltd. that incorporates secure encryption in the device itself on a time-limited basis.

Mobile Devices

- Mobile devices which are the property of EVAT must be enrolled on the MDM security system. Unauthorised removal of security profile may result in the loss of privileged use.
- If a device becomes lost or inaccessible, this may involve IT 'remote wiping' the device to ensure that EVAT data is no longer available. This 'remote wiping' of the device may remove user data, EVAT takes no responsibility for user data lost in this circumstance.
- All mobile devices must be secured using a 4-digit PIN. This must not be disclosed to anyone.

The Trust may exercise its right by electronic means to monitor the use of the Trust's computer systems, including the monitoring of websites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Trust's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Staff Agreement

I have read and understand the Trust rules for this Acceptable Use Agreement. I will use the Trust computer network system and the internet in a responsible way and observe all the restrictions explained to me by the Trust.

Forename: Surname: (In Block Capitals)

Job title:

Staff Signature

Date / /

THIS FORM TO BE RETURNED TO PRINCIPALS.

OFFICE USE ONLY

Staff Pay Roll Number (if available): Supply Teacher ☐

IT SYSTEMS USE ONLY

Network ☐ Spreadsheet ☐ VLE ☐

Computer Viruses

- All files downloaded from the internet, received via email or on removable media such as a memory stick must be checked for any viruses using Trust provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on Trust ICT equipment.

- If your machine is not routinely connected to the Trust network, you must make provision for regular virus updates through IT Systems.

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

Data Security – this section should be read in conjunction with the Trust Data Protection Policy

- The Trust gives relevant staff access to its Management Information System (SIMS), with a unique username and password.

- It is the responsibility of everyone to keep passwords secure

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

- Staff keep all Trust related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should leave any portable or mobile ICT equipment or removable storage media in unattended vehicles. Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under control at all times

- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

Disposal of ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written

guarantee that this will happen.

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  Data Protection Act 1998 and GDPR 2018
  Electricity at Work Regulations 1989

- The Trust will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

- The Trust's disposal record will include:

    - Date item disposed of
    - Authorisation for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media *
    - How it was disposed of e.g. waste, sale
    - Name of person & / or organisation who received the disposed item

  * If personal data is likely to be held the storage media will be physically destroyed to ensure the data is irretrievable.

- Any redundant ICT equipment being considered for sale will have been subject to a recent electrical safety check and hold a valid PAT certificate

Email

The use of email within across the Trust is an essential means of communication for both staff and pupils. In the context of the Trust, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally.

Staff, Directors and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors and staff are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of our safeguarding agenda.

Managing Email

- The Trust gives all staff their own email account to use for all Trust business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

- Staff should use their Trust email for all professional communication.

- The Trust requires all users to include an email signature and company information in all emails in the following format (this should be school specific).

Name
Role
The Education Village Academy Trust
Salters Lane South
Darlington
DL1 2AN
T: 01325 254000
www.evat.org.uk

The Education Village Academy Trust
Where learning has no limits

The Education Village Academy Trust is an exempt charity. It is a company limited by guarantee in England and Wales. Company No 7748248. Registered office address: The Education Village, Salters Lane South, Darlington, DL1 2AN.

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

- Under no circumstances should staff contact pupils, parents or conduct any Trust business using personal email addresses.

- All emails should be written and checked carefully before sending, in the same way as a letter written on academy/school/Trust headed paper.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- Emails created or received as part of your Trust role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

  – Delete all emails of short-term value

- Organise email into folders and carry out frequent house-keeping on all folders and archives

- All student email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.

- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email and include on the e-safety log.

- Staff must inform their line manager if they receive an offensive email who will ensure it is logged.

- However you access your Trust email (whether directly, through webmail or 'Anywhere' when away from the school site or on non-school hardware) all the school email policies apply.

Sending emails

- Use your own school email account so that you are clearly identified as the originator of a message

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate. Only use the ALL STAFF email groups if absolutely necessary.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

  School email is not to be used for personal advertising.

Receiving emails

- Staff should check their email regularly – usually at least twice a day.

- Staff should activate their 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; consult your network manager first

- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

  The automatic forwarding and deletion of emails is not allowed

E-Safety – Roles and Responsibilities

E-Safety is an important aspect of strategic leadership within our Trust. The Chief Executive and Board of Directors have ultimate responsibility to ensure that the

policy and practices are embedded and monitored. Each academy/school has a named e-Safety co-ordinator and Safeguarding linked governor.

Haughton Academy: Andrew Hinnigan
Beaumont Hill Academy: Adrian Lynch
Springfield Academy: Richard Gartland
Gurney Pease Academy: Alison Sinclair
Marchbank Free School: Andy Emmerson
Overall Trust responsibility: Mike Butler

All members of the Trust community have been made aware of who holds these posts. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance.

Academy/school staff and governors are updated by the Principal / e-Safety co-ordinator and all governors have an understanding of the issues and strategies in their school/academy in relation to local and national guidelines and advice.

This policy, supported by the Trust's acceptable use agreements for staff, governors/directors, visitors and students, is to protect the interests and safety of the whole Trust community. It is linked to the following Trust policies: child protection, health and safety, home-school agreements, and behaviour policy.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The academies and schools in the Trust provides opportunities within a range of curriculum areas to teach about e-Safety.

- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety and PSHE curriculum and is delivered in an age appropriate manner.

- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them. All information shared with students is age appropriate.

- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities. All information shared with students is age appropriate.

  Students are 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 the 'CEOP

report abuse' button. All information shared with students is age appropriate.

E-Safety training for staff

- Trust staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages.
- New Trust staff receive information on the Trust's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see e-Safety Co-ordinator section)

  All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

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 Trust's Deputy Chief Executive or school/academy e-Safety co-ordinator. 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 IT Systems via the IT Helpdesk and logged.

E-Safety Incident Log

Trust e-Safety co-ordinators should keep a log of any incidents to ensure appropriate action is taken and any trends or specific concerns are identified.

Each school/academy in the Trust should have a separate log and will be reported at each ESC meeting.

Example Log:

Date & Time	Name of pupil/staff	Room and device	Details of incident	Action taken

Internet Access

The internet is an open worldwide communication medium, available to everyone, 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. All internet use through the Trust network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected or suspected it will be followed up.

- The Trust provides students and staff with supervised (filtered) access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites, online services, software and apps before use.
- Searching for images through open search engines is discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Users must not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- All web access across the Trust benefits from a monitored service. Staff and students are aware that email and internet activity can be monitored and explored further if necessary.

Managing online technologies

Online technologies, 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 pupils to think carefully about the way that information can be added and removed by all users, including themselves,

from these sites.

- The Trust endeavours to deny access to social networking and online games websites to pupils within school.

- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are. All information shared with students is age appropriate.

- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites 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 websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

- Students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.

- Students are asked to report any incidents of Cyberbullying to their class teacher or e-Safety co-ordinator.

  Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the Trust VLE (Frog) or other systems approved by the school/academy Principal.

Parental involvement

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their student on admission to the school.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website and on the VLE)

- Parents/carers are expected to sign a Home School agreement/AUP with their child.

- The Trust disseminates information to parents relating to e-Safety where appropriate through:

  - Information evenings
  - Practical training sessions e.g. current e-Safety issues
  - Posters
  - School website information
  - Newsletter items

Passwords

- **Minimum Password Length = 8 characters**
  The minimum length a password needs to be before the system will accept it.
- **Maximum Password Age = 2 months**
  After the defined number of days, the password will need to be reset in favour of a new one.
- **Password Complexity = Enabled**
  All passwords MUST have complexity such as uppercase letters, numbers and/or symbols.
- **Minimum Password History Length = 12 Months**
  Passwords when reset must not be the same as previous passwords within the last 12 months.
- **Lockout Threshold = 5 Attempts**
  Incorrect password attempts exceeding the threshold will lock the account out to prevent unauthorised access.
- **Lockout Observation Window = 10 Minutes**
  Incorrect password attempts will be reset within 10 minutes preventing a lockout.
- **Lockout Duration = 1 day**

  A lockout condition will last for 1 day unless unlocked by a member of the EdIT Learning team.

Always use your own personal passwords

- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures. Staff should change temporary passwords at first logon.

- Do not record passwords or encryption keys on paper or in an unprotected file.

- Only disclose your personal password to authorised EdIT Learning team when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

- Never tell a child or colleague your password.

Protecting sensitive data

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure that personal, sensitive or confidential information is not disclosed to any unauthorised person.
- Sensitive information must not be posted on the internet, or disseminated in any way that may compromise its intended restricted audience.

  Keep your screen display out of direct view of any third parties when you are

accessing personal, sensitive, confidential or classified information.

Storing and transferring data using removable media

- Staff must not use removable data storage media (e.g. USB sticks, portable hard drives) to transfer data between their place of work and home (or any other remote location).

- In the most exceptional one-off circumstances, and only at the discretion and with the written permission of either a Principal or the Chief Executive, removable data storage media provided by EdIT Learning Ltd. that incorporates secure encryption in the device itself may be used on a time-limited basis.

- Securely dispose of removable media that may hold personal data.

Using remote access

- You are responsible for all activity via your remote access facility.

- Only use equipment with an appropriate level of security for remote access.

- To prevent unauthorised access to school systems, keep passwords secure.

- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

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 a non-school environment.

Safe use of images

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils. This includes when on educational visits.

- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others.

Pupils and staff must have permission from the academy/school Principal before any image can be uploaded for publication.

The Trust may place a photo of a student with first name and first letter of the surname on Apps for use by parents, on walls in Academies or publications such as Academy Newsletters.

Publishing images and work

On a child's entry to the academy/school, 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.
- on Twitter, Facebook or other official Trust social media sites.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/ transmitted on a video or webcam.
- on the Trust's Virtual Learning Environment (Frog) or Tapestry (Beaumont Hill Academy).
- in display material that may be used in the academy/school's communal areas.
- in display material that may be used in external areas, i.e. exhibition promoting the academy/school.
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form (see appendix 1) is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the Trust.

Other than on the VLE (which is password protected) pupils' full names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting pupil work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Once this has been granted, the pupils first name and initial should be used and not their full name.

Only authorised staff have the authority to upload to the internet and Trust website. See the EVAT Website Management Strategy document.

The Trust will also seek permission from staff to use their image. A similar consent form will be used (see Appendix 2).

In BHA Tapestry is used with certain individual students. The security credentials are noted in Appendix 3 whilst the consent letter is Appendix 4.

Storage of images

- Images/ films of children are stored on the school's network and Trust owned devices such as iPads.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks).
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource such as the VLE.

CCTV

The Trust use CCTV for security and safety. The system is controlled and managed by Mitie in line with the PFI contract. Access to recorded images on the system is limited to:

- Mitie PFI management (EV)
- EVAT Executive Leadership Team
- EVAT Premises and H&S Manager
- IT Systems & Media Manager

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school/academy.
- All students are supervised by a member of staff when video conferencing.
- Approval from the academy/school Principal is sought prior to all video conferences within school to end-points beyond the school/academy.
- Any Trust 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 written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Trust IT equipment

- As a user of Trust ICT equipment, you are responsible for your activity.
- IT Systems log ICT equipment issued to staff and record serial numbers as part of the Trust's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the Trust's network. You are responsible for the backup and restoration of any of your data that is not held on the Trust's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device.
- Privately owned ICT equipment should not be used on the Trust network.
- On termination of employment, resignation or transfer, all ICT equipment must be returned to your Line Manager. You must also provide details of all your system logons so that they can be disabled. This will be checked during your exit interview.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

  All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile IT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on Trust systems and hardware will be monitored in accordance with the general policy.

- Staff must ensure that all Trust data is stored on the Trust network, and not kept solely on a laptop or tablet. Any equipment where personal data is likely to be stored must be encrypted.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

- Ensure portable and mobile ICT 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 IT Systems, fully licensed and only carried out by your IT technicians.

- In areas where there are likely to be members of the general public, portable or mobile ICT 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.

Personal mobile devices

- The Trust allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Trust allow a member of staff to contact a pupil or parent/ carer using their personal device.

- Students are allowed to bring personal mobile devices/phones to school but must not use them in the school buildings. At all times the device must be switched onto silent. Please note, Beaumont Hill Academy students are not permitted to bring mobile devices onto the school site at all.

- The Trust is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any members of the Trust community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the Trust community.

- Users bringing personal devices into an academy/school must ensure there is no inappropriate or illegal content on the device.

Trust provided mobile devices

- The sending of inappropriate text messages between any members of the Trust community is not allowed.

- Where the Trust provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

Where the Trust provides a laptop for staff, only this device may be used to conduct Trust business outside of the school/academy.

Servers

- Servers are kept in a locked and secure environment.

- Limit access rights to senior IT staff only.
- Servers are always password protected and locked.
- Servers have security software installed appropriate to the machine's specification.
- Backup tapes are encrypted using appropriate software.
- Data is backed up regularly.
- Backup tapes/discs are securely stored in a fireproof container.

Back up media stored off-site is secure.

Social Media

This statement should be read in conjunction with the Trust's Staff Social Media Policy.

- Academies and schools in the Trust uses Facebook and Twitter to communicate with parents and carers. Principals are responsible for all postings on these technologies and monitor responses from others.
- Staff are not permitted to access their personal social media accounts using school equipment at any time during school hours.
- Students are not permitted to access their social media accounts whilst at school.
- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

  Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

E-Safety Governance

Education Standards Committee (ESC) members' passwords will be renewed annually. When the passwords have expired members will be required to select a new password that conforms to the complexity requirements.

An EVAT emails and secure access (portal) has been set been up to enable ESC members to read and view papers. Access to this is limited to individuals who have been provided with suitable credentials.

ESC members using their own devices at home are responsible for ensuring screens are locked and ensuring they abide by the principles of data sharing ie that the information shared is necessary for the purpose for which you it is being sharing it, is shared only with those individuals who need to have it.

Member's passwords will automatically expire every 365 days at which time a new one will be required.

- **Minimum Password Length = 8 characters**
  The minimum length a password needs to be before the system will accept it.
- **Maximum Password Age = 2 months**
  After the defined number of days, the password will need to be reset in favour of a new one.
- **Password Complexity = Enabled**
  All passwords MUST have complexity such as uppercase letters, numbers and/or symbols.
- **Minimum Password History Length = 12 Months**
  Passwords when reset must not be the same as previous passwords within the last 12 months.
- **Lockout Threshold = 5 Attempts**
  Incorrect password attempts exceeding the threshold will lock the account out to prevent unauthorised access.
- **Lockout Observation Window = 10 Minutes**
  Incorrect password attempts will be reset within 10 minutes preventing a lockout.
- **Lockout Duration = 1 day**

  A lockout condition will last for 1 day unless unlocked by a member of the EdIT Learning team.

Public Sector Equality Duty (Equality Act 2010)

In preparing or amending this policy, the author has given due regard to the Public Sector Equality Duty; that is they have considered any potential impact on people who share certain protected characteristics. These protected characteristics are defined as: race, disability, sex, age, religion or belief, sexual orientation, pregnancy and maternity and gender reassignment.

Appendix 1

Photo consent form

I understand and consent that the Trust may hold a photo of my child on a secure database for identification purposes.

Please tick one of the boxes below to give or withhold consent for wider use of your child's photo:

☐ I give consent for my child's photograph to be used in both internal and external media publications, social networks (e.g. the Academy Facebook page) and other publicity materials. Their picture may also be used in displays in the Academy classroom or on walls in the Academy.

☐ I DO NOT wish my child's photograph to be published internally or externally.

Parent/carer signature	
Parent/carer name	
Pupil name	
Academy name	
Date	

Appendix 2

Staff photo consent form

Please tick one of the boxes below to give or withhold consent for the taking and use of your photo:

☐ I give consent for my photograph to be used in both internal and external media publications, social networks (e.g. the Academy Facebook page) and other publicity materials. Your photo may also be displayed on noticeboards in the Academy.

☐ I DO NOT wish my photograph to be published internally or externally.

Name	
Signature	
Academy/TST	
Date	

Appendix 3

Statement of security from Tapestry.

Tapestry, and have gone to great lengths to ensure data is stored securely and protected from unauthorised access. Some of the measures taken include:

Physical security

- Hosted on dedicated servers in a high security data centre in the UK (just north of London). Knowing that the data (and backups) are not stored in other jurisdictions means that we can be confident that all data is governed by UK law.
- These servers are backed up four times daily, to an off-site datacentre 20 miles from our main datacentre, so that in the event of a major disaster, recovery of entire servers is still possible within a couple of hours.
- The servers are proactively managed 24 hours a day, including regular updates and patches for security vulnerabilities.
- Additionally, our servers conform to very high environmental standards, being audited and certified to ISO 14001 (Environment Management) standards.

Application Security

- The Tapestry accounts and code are held on a secure server (https and the padlock on the address bar) as is usual for sites requiring extra security.
- Each Tapestry account has its own database - a setting's information is not held in a larger database with other accounts.
- The code itself is developed using hack resistant techniques such as CSRF (Cross Site Request Forgery) protection via form keys, and input fields checked and stripped for XSS (Cross Site Scripting) data and characters
- Filenames are encoded for uploaded photos, video and images
- Log in passwords are never stored but are instead salted and then hashed
- The framework is well tested and developed by a programmer experienced *in the field of web applications subject to hacking attempts*

The Education Village Academy Trust
Beaumont Hill Academy

Salters Lane South, Darlington, County Durham DL1 2AN
T: 01325 254000 **F:** 01325 254222
E: admin@educationvillage.org.uk

www.educationvillage.org.uk

Appendix 4

Tapestry Online Learning Journal Permission

Please complete the following permission.

Pupil's Name . . . . . .

1) I agree to my child having a Tapestry Online Learning Journal.

2) I give permission for my child's image to appear in photographs/videos in other children's learning journey. (We try to avoid this but it is not always possible when children are working so closely together).

3) I consent to treat photographs containing images of other children as for my own personal use only. (This means that the information cannot be shared with others, or published in any way, without the explicit consent of the parents or carers of those children who may be included. For example, any such photographs **cannot** be posted on a social networking site or displayed in a public place).

Parent Signature.....

Date.....

I would/ I would not like to access my child's Tapestry Online Learning Journal.

The e-mail address I would like to link with the account so I have access to my child's Online Learning Journal is:

Email address. . . . . .