Reviewed October 2017

Eastbrook School

e - safety

Policy

e-safety Policy

Introduction

Eastbrook School recognises that ICT in the 21st Century is 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 safe and effective use of these technologies in order to provide our young people with the skills to access life-long learning, employment and safe communication.

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
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Webcams
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst much ICT is exciting and beneficial both in and out of the context of education, particularly web-based resources, it cannot be consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At Eastbrook School we protect wherever possible and appropriate.

However, the main focus of our approach is to prepare our students to protect themselves.

At Eastbrook School**,** we understand the responsibility to educate our students 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.

Both this policy and the **Acceptable Use Agreement** (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, personal digital assistants [PDAs], tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc). Please refer to the guidance on our school website for more information about online safety.

Monitoring

The Headteacher, Network Manager, Business Manager or Deputy Headteacher – may inspect any ICT equipment owned or leased by the School at any time without prior notice.

The Network Manager may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving the school's students, 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; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

The Network Manager may under instruction from the Headteacher, 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 their school account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff, under the direction of the Headteacher, and comply with the Data Protection Act 1998, 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 School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure and will be reported to the Headteacher.

Policy breaches may also lead to criminal or civil proceedings as appropriate.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Network Manager and e-safety Co-ordinator (the Headteacher).

Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Network Manager.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them
- No-one apart from the Network Manager should interfere with any anti-virus software installed on school ICT equipment
- If a machine is not routinely connected to the school network, you must make provision for regular virus updates through the Network Manager
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Network Manager immediately. You will be advised as to what actions to take and you should advise others that need to know

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 all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- 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

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

On admission parent / carers are provided with the opportunity to refuse consent (on behalf of students) for the appropriate taking of images by staff and students with school equipment to be used within the school or in promotion of the school's activities.

On induction staff are provided with the opportunity to refuse consent for the appropriate taking of images by staff and students with school equipment to be used within the school or in promotion of the school's activities.

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the student attends this school unless there is a change in circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be withdrawn by the parent with parental responsibility for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. e-mail and postal addresses of students will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Staff and students are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of staff or student in school or on school trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

Storage of Images

- Images/ films of students are stored on the school's network
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform
- The School has the responsibility of deleting the images when they are no longer required, or the student has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Senior Team, Network Manager and On Call Support Worker. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, and under staff supervision
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

Video Conferencing

- All students are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- Participants in conferences offered by 3rd party organisations may not be CRB checked – but they will not be in direct unsupervised contact with Students

- 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

School ICT Equipment including portable and mobile ICT equipment and removable media

- All school users of ICT are responsible for any activity undertaken on the school's ICT equipment provided
- Eastbrook School log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- We do not allow visitors to plug their ICT hardware into the school network points (unless special provision has been made). They are directed to the wireless ICT facilities or provided with school hardware
- All ICT equipment that used is kept physically secure

- We abide by the Computer Misuse Act 1990
- The School's network drive is backed up each day.
- Personal or sensitive data is not stored on the local drives of desktop PCs.
- A time locking screensaver is applied to all machines. All PCs etc accessing personal data have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, all ICT equipment is returned to the Network Manager.
- It is the user's responsibility to ensure that any information accessed from a PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the Headteacher
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

This section covers such items as laptops, PDAs 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 School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted if taken off the school site.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes.
- 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 the Network Manager, fully licensed and only carried out by your ICT Support
- 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

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for students. 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 school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal and School Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times they should not be seen or heard in the school buildings.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any 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

Removable Devices

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the Network Manager

Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data. CMIS Database Servers installed by SITSS since April 2009 are supplied with encryption software.
- Servers are in a locked and secure environment
- Access rights are limited
- The server is password protected and locked
- Existing servers have security software installed appropriate to the machine's specification
- Back up tapes are encrypted by appropriate software
- Data is backed up regularly
- Back up tapes/discs are securely stored in a fireproof container
- Back up media stored off-site is secure
- Remote back ups are automatically securely encrypted.

Systems and Access

- All staff are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC
- Users are instructed not to allow any unauthorised person to use school ICT facilities and services that have been provided to themUsers use only their own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Users are advised to keep the screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- All screens have an automatic lock to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Users are advised to logoff from the PC completely when going to be away from the computer for a longer period of time
- Users are instructed that it is imperative that they do not access, load, store, post or send from school 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 school or Local Authority into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school'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 Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, we obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. The Network Manager must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others
    2. They are not for profit or to premium rate services
    3. They conform to this and other relevant Local Authority and school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times
- Follow the appropriate procedures in the event of receiving a telephone call containing a threat.

Mobile Phones

- You are responsible for the security of your school mobile phone. Report the loss or theft of any school mobile phone equipment immediately
- The school 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 school mobile phone prior to using it
- You must not send text messages to premium rate services
- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad.
- Never use a hand-held mobile phone whilst driving a vehicle. Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-safety coordinator any issue of e-safety that concerns them

There will be an on-going opportunity for staff to discuss with the Headteacher any issue of data security that concerns them

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been read, amended and approved by the staff, head teacher and governors.

Eastbrook School

Acceptable Use Agreement: 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 technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- 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 inline with school policy and not be distributed outside the school network without the permission of the Headteacher.
- 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 Eastbrook School into disrepute.
- 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.

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 e-safety 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 tutor, Head of Year or a member of the Senior Leadership Team.

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 e-safety rules and to support the safe and responsible use of ICT at Eastbrook School.

Parent/ Carer Signature ……..……

Student Signature……..

Form …… Date ……

Eastbrook School

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

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. 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 school e-safety coordinator (the Headteacher) or Lin Southan (Business Manager).

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- 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 give out my own personal details, such as personal mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of 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.
- Images of students and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- 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 Headteacher.
- 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, or the school, into disrepute.
- I will support and promote the school's e-safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.

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

Signature …….…….…… Date ……

Full Name …….....(printed)