The Boston Witham Academies Federation

E Safety

Introduction and Aims

The purpose of this policy is to establish the ground rules we have for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and learners learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and out of school has been shown to raise educational standards and promote learner achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with the following:

- Anti-Bullying Policy
- Behaviour for Learning Policy
- Code of Conduct Policy
- Child Protection Policy

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build learners' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The academy provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the academy intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

This policy applies to all members of the academy federation (including staff, learners, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of the academy. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the academy. The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school and will impose sanctions and refer to police where necessary.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the academy:

The governors will ensure that this policy will be reviewed and monitored annually.

The CEO will ensure that the federation has a nominated person as E-safety Co-ordinator (a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of cyberbullying incidents).

Staff will familiarise themselves with this e-safety policy and procedures.

The Chief Executive Officer is responsible for ensuring:

- The safety (including e-safety) of all members of the academy community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The school's Designated Child Protection Officers should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Ensure reports of e-safety incidents are logged to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in the academy

Network manager

The Network manager is responsible for ensuring that:

- The academy's ICT infrastructure is secure and meets e-safety technical requirements
- The academy's password policy is adhered to
- The academy's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Manager keeps up to date with e-safety technical information
- The use of the academy's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

Teaching & Support Staff

All teaching and support staff are responsible for ensuring that:
- They have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- E-safety issues are embedded in all aspects of the curriculum and other academy activities
- Learners understand and follow the academy's e-safety policy

- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Learners (to an age appropriate level)

- Are responsible for using the school ICT systems and will be required to sign our Internet and Acceptable Use Policy before being given access to academy systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the academy's e-safety policy also covers their actions out of school, if related to their membership of the school. Inappropriate use of social media in and out of the academy may lead to sanctions being imposed.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The academy will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the ICT Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant academy Acceptable Usage Policy.

Education and Training

E-safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the curriculum and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Learners are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Learners are helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Learners are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in the academy

- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- Staff are issued with the AUP annually

Copyright

- Learners to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Learners are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

Staff Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Commmunication

Email

- Digital communications with learners (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official academy systems (see staff guidance in child protection policy).
- The academy's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);
- Under no circumstances should staff contact learners, parents/carers or conduct any academy business using their own personal e-mail addresses.
- Academy e-mail is not to be used for personal use. Staff can use their own email in the academy (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ children.

Mobile Phones

- **Academy** mobile phones only should be used to contact parents/carers/learners when on academy business with learners off site. Staff should not use personal mobile devices.
- **Staff** should not be using personal mobile phones in the academy during working hours when in contact with children.
- Learners should adhere to the rules and guidelines regarding mobile phone use in the academy.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, learners, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Learners/Parents/carers** should be aware the academy will investigate misuse of social networking if it impacts on the well-being of other learners or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary and sanctions will be imposed. Where the abuse is bullying or racism this will also trigger sanctions under those policies.
- Learners will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our learners. A list is published to all staff, but can also be obtained from the Head of Academy or the designated child protection officer in the academy.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Head of Academy or the ICT co-ordinator.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the academy will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The academy has an active website which is used to inform, publicise academy events and celebrate and share the achievement of learners.

Removable Data Storage Devices

- *Only school provided removable media should be used*
- All files downloaded from the Internet, received via e-mail or provided on removable media (eg. CD, DVD, USB flash drive, memory cards etc) must be checked for viruses using academy provided anti-virus software before run, opened or copied/moved on to local/network hard disks.
- Learners should not bring their own removable data storage devices into the academy unless asked to do so by a member of staff and it has been approved by the IT team. Any such device should be used solely for learner work and not to bring in games etc

Websites

- In lessons where Internet use is pre-planned, learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger learners who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which learners are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the learners on the internet by the member of staff setting the task. All staff are aware that if they pass learners working on the internet that they have a role in checking what is being viewed. Learners are also aware that all internet use at school is tracked and logged.
- The school only allows the E-Safety Co-ordinator, ICT co-ordinator and SLT to access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Learners

- Learners should never, under any circumstances, share their password or account.
- Inform staff immediately if passwords are traced or forgotten.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the academy's network without the specific permission of the Head of Academy or Network Manager.
- Learners should not bring in their own equipment unless asked to do so by a member of staff.

Use of Academy Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously or Windows key + L) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the academy's Internet access is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator or members of the Senior Leadership Team depending on the severity of the incident.

- E-Safety Coordinator and Network Manager will log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the academy who comes across an e-safety issue does not investigate any further but immediately reports it to the E-safety Co-ordinator or Head of Academy and impounds the equipment. This is part of the academy safeguarding protocol. (If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Head of Academy).

Responding to incidents and reporting

Any e-safety incidents must immediately be reported to the Head of Academy (if a member of staff or learner) or the E-Safety Coordinator who will investigate further following e-safety and safeguarding policies and guidance.

- Staff should keep any records of the abuse – text, e-mails, voice mail, web site or instant message. Screen prints of messages or web pages should be taken and time, date and address of site should be recorded.
- Staff should inform the nominated person of incidents at the earliest opportunity.
- Monitoring and confiscation must be appropriate and proportionate.
- Where a potential criminal offence has been identified, and reported to the police, the federation will ensure that any internal investigation does not interfere with police inquiries.

- Where learners are found to have made unfounded, malicious claims against staff members, relevant and appropriate disciplinary processes will be applied.
- Staff should report all incidents to the nominated person. The nominated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

Action for Inappropriate Use of Social Networking Sites

Following a report of inappropriate use of social networking sites, the nominated person will take the following action:

- Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed.
- If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. The material posted may breach the service provider's terms and conditions of use and can then be removed.
- In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.
- Before the nominated person contacts a service provider, he or she will check the location of the material – for example by taking a screen capture of the material that includes the URL or web address. If the nominated person is requesting that the service provider takes down material that is not illegal, he or she will be clear how it contravenes the site's terms and conditions.

Sanctions for members of the federation community (including parents/carers) the federation will:

- deal with harassment and bullying under the relevant federation procedure e.g. through disciplinary action if appropriate;
- take care to make an informed evaluation of the severity of the incident;
- deliver appropriate and consistent sanctions; and
- provide full support to the staff member(s) affected.

The governors recognise their legal duty to protect staff from unlawful harassment as well as mental and physical injury at work.
In cases of potentially criminal content, the nominated person will consider whether the police should be involved, following appropriate liaison with staff, and parents where necessary.

Review July 2019

APPENDIX 1

USEFUL INFORMATION FOR NOMINATED E-SAFETY LEADS

Mobile Phones

All UK mobile phone operators have nuisance call centres set up and/or procedures in place to deal with such instances. They may be able to change the number of the person being bullied. Mobile operators cannot bar a particular number from contacting a phone, but some phone handsets do have this capacity. Action can be taken against the bully's phone account (e.g. blocking their account) only with police involvement.

Contacts:

O2: ncb@o2.com or 08705214000.

Vodafone: 191 from a Vodafone phone or 08700700191 for Pay Monthly customers and 08700776655 for Pay as you Go.

3: Call 333 from a 3 phone or 08707330333.

Orange: Call 450 on an Orange phone or 07973100450 for Pay as you Go, or 150 or 07973100150 for Pay Monthly.

T-Mobile: Call 150 on a T-Mobile phone or 08454125000.
A list of service providers is attached at Appendix 2.

Virgin: Call 789 from a Virgin phone or 0845 6504500.

EE: Use the 7726 service to register a complaint for automated or unsolicited marking voice calls. You need to text the word call followed by the number which called you to 7726. Contact the Information Commissioner's Office (ICO) on 0303 123 1113 to complain.

Social networking sites (e.g. Bebo, FaceBook, MySpace)

Contacts of some social network providers:

Facebook: Reports can be made by clicking on the `Report' link located on pages throughout the site. Facebook users can also report another user by using the "Report/Block" link that appears at the bottom of a user's profile page or by listing the user's name in the "Block List" box that appears at the bottom of the Privacy page.

MySpace: Reports can be made by clicking on the `Contact MySpace' link at the bottom of every MySpace page and selecting the `Report Abuse' option. Alternatively, click on the `Report Abuse' link located at the bottom of each user profile page and other user-generated pages. Inappropriate images can be reported by clicking on the image and selecting the `Report this Image' option. Additionally, federation staff may email MySpace directly at schoolcare@myspace.com
www.myspace.com/safety

Snapchat: Reports can be made by accessing the Snapchat help page https://support.snapchat.com; Unwanted users can be removed – use the support page for added guidance.

Video and photo hosting sites

YouTube: Logged in YouTube members can report inappropriate content by using the `flag content as inappropriate' function which appears under every video.

Flickr: Reports can be made via the `Report Abuse' link which appears at the bottom of each page. Logged in members can use the `flag this photo' link to report individual pictures. www.flickr.com/guidelines.gne

OoVoo: to report inappropriate content make sure you block the user and contact OoVoo using the following link:
http://support.oovoo.com/ics/support/ticketnewwizard.asp?style=classic

You should also make sure your privacy settings are appropriately set, you can do this with the following link:
http://support.oovoo.com/link/portal/3908/4244/ArticleFolder/169/Privacy-Security

WhatsApp: to report inappropriate content in WhatsApp you need to block their content which then flags them up to WhatsApp, scroll all the way to the top of the chat history and on the left hand side there three options – block, edit and add – you will need to select block.

Instagram: Logged in users can view supporting material for instagram from the prided link https://help.instagram.com/

Instant Messenger

It is good practice for Instant Messenger (IM) providers to have visible and easy-to-access reporting features on their services. Instant Messenger providers can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations, and most IM providers allow the user to record all messages.

Contacts of some IM providers:

Yahoo!: When in Yahoo! Messenger, clicking on the `Help' tab will bring up a range of options, including `Report Abuse'.

Chatrooms, individual website owners/forums, message board hosts

It is good practice for chatroom providers to have a clear and prominent reporting mechanism to enable the user to contact the service provider. Users that abuse the service can have their account deleted. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use.

APPENDIX 2

How to Stay 'Cybersafe' – Do's and Don'ts

Staff should:

- not post information and photos about themselves, or federation -related matters, publicly that they wouldn't want employers, colleagues, learners or parents to see;
- keep passwords secret and protect access to accounts;
- not "befriend" learners or parents/carers on social networking sites. (If staff are related to learners and parents /carers and wish to have them as "friends" they should let federation management know if they decide to do this);
- be strongly advised to think carefully about "befriending" ex-learners as they may still have siblings or other contacts in the federation. (If staff are related to ex-learners and wish to have them as "friends" they should let federation management know if they decide to do this.);
- keep personal phone numbers private and not use their own mobile phones to contact learners or parents;
- use an academy mobile phone when on an academy trip;
- keep a record of their phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on academy premises and report thefts to the police and mobile operator as soon as possible;
- ensure that federation rules regarding the use of technologies are consistently enforced;
- not personally retaliate to any incident;
- report any incident to the appropriate member of staff in a timely manner;
- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material, including the URL or web address.
- use federation e-mail addresses only for work purposes.
- be aware that if they access any personal web-based e-mail accounts via their academy network, that these may be subject to the federation's internet protocol which could include monitoring and surveillance.

E Safety – Illegal and Inappropriate Activity Flow chart

The Boston Witham Academies Federation