Foundation Academies Trust

E - SAFETY POLICY

Date Reviewed: November 2019 by Stacey O'Connor (Essa Academy DSL)

Next Review: December 2020

Microsoft Office User

Foundation Academies Trust

CONTENTS

Role and responsibilities

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at ESSA trust with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff at the academy.
- Assist staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows: Content

- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.
- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.

Contact: Grooming, cyber-bullying in all forms and identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords.

Conduct: Privacy issues, including disclosure of personal information, digital footprint and online reputation. Health and well-being is also a factor (amount of time spent online (Internet or gaming). As well as sexting (sending and receiving of personally intimate images).

Communication: Policy to be posted on the school website, to be part of school induction pack for new staff. Staff and students are aware of the expectations of the academy and agreements in place.

Educations and curriculum

This school has a clear, progressive e-safety education programme as part of the Computing curriculum and PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- STOP and THINK before they CLICK: to develop a range of strategies to evaluate and verify information before accepting its accuracy.
  To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what you understand how search engines work and to understand acceptable behaviour when using an online environment /
- email, i.e. be polite, no bad or abusive language or other inappropriate.

- Attracting the wrong sort of attention: understanding why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments. Also to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos.
- Permission: to know not to download any files – such as music files - without permission
- Other areas that could be potentially dangerous: Grooming, sexting and so on. Students will receive in depth information on this in weekly British Values and PSHE sessions.

Incident management

Expected conduct: Staff are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand-held devices. Students should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. Parents/Carers should give consent for students to use the Internet, as well as other technologies, as part of the Acceptable Use Agreement at the time of their child's entry to the school.

Throughout the academy there is strict monitoring and application of the e-safety policy and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions. Monitoring and reporting of e- safety incidents takes place through CPOMS and contribute to developments in policy and practice in e-safety within the academy. The records are reviewed/audited and reported to the school's senior leaders and E-Safety Governors.

Managing ICT and Data security

Internet access, security (virus protection) and filtering

This school has a dedicated, uncontended leased line providing internet connectivity, which is secured by a local firewall and onsite filtering solution. Systems we use blocks sites that fall into categories such as pornography, race hatred, gaming sites with terrorist and extremist material, and sites of an illegal nature, etc. All Chat rooms and social networking sites are blocked except those that are part of an educational network or approved Learning Platform. All users have been informed that Internet use is monitored daily/weekly with notifications going straight to the Principal.

Staff and students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator logs or escalates as appropriate to the Technical service provider or LA as necessary.

Advise and information on reporting offensive materials, abuse/ bullying etc is available for students, staff and parents and also the dangers of this. All students have their own unique username and password which gives them access to the Internet, the VLE and their own school approved email account. It is clear that no one should log on as another user and that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network. All users are required to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

Staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities.

Password policy: It is clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private. We require staff to change their passwords into the system every 90 days.

E-mail: We provide staff with an email account for their professional use and makes clear personal email should be through a separate account. Staff should not publish personal e-mail addresses of students or staff on the school website. ESSA will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.

Students: Students are taught about the safety of using e-mail in school. They must not reveal private details of themselves or others in e-mail, such as address, telephone number and any other personal details

Staff: Staff only use the e-mail system for professional purposes. Access in school to external personal email accounts may be blocked. Never use email to transfer staff or student personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer). Staff know that e-mail sent to an external organisation must be written carefully and professional at all times.

School website: The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

Social networking: Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students. If staff do know or are related to students of previous students it is expected for staff to inform the DSL so they are aware and discuss any potential issues that may arise as good practice and to safeguard themselves.

CCTV: We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any without permission except where disclosed unless there is an incident involving the Police as part of a criminal investigation.

Strategic and operational practices

We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services. Staff with access to setting-up usernames and passwords for email, network access and VLE access are working within the approved system and follow the security processes required by those systems. We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

We require staff to log-out of systems when leaving their computer, but also enforce lock- out after 30 minutes idle time. We use the DfE S2S site to securely transfer CTF student data files to other schools.

Equipment

Students using the devices owned by school (e.g. IPads/laptop/notebook/voting devices) must adhere to the protocols for using such devices. The member of staff supervising the activity must ensure that they completes the record sheets showing which students has been issued with which device and is responsible for collecting the devices in a safe manner at the end of the activity. Where a device is damaged or stolen, the record sheets will be examined to see who the device had been issued to. Any student found to have deliberately damaged a device will be dealt with in accordance with the behaviour Policy and will be issued with a bill to cover the financial cost of the repair or re-purchase. If parents have financial difficulties a payment plan can be put in place. However if family do not support this agreement this could potentially delay their child from returning into circulation pending investigation until an agreement has been made with the school.

If a member of staff is found to have breached the protocols and thus to have been responsible for any damage or theft, their Curriculum Leader will be issued with a bill to cover the cost of repair or re-purchase.

Personal mobile phones and mobile devices

Mobile phones brought into school are entirely at the staff member, students' & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held / electrical device brought into school students have the opportunity to hand them belongs over to prevent incidents like this occurring.

Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day and they have left the building. Students who do not adhere to this will have items confiscated and placed with a senior leader or pastoral lead. Staff have the right to keep this until a parent/carer collects this item it is at their discrepancy individual circumstance's will be dealt on a case-by-case basis. Students failing to hand over items will lead to further sanctions linking to our other policies for sanctioning and behaviour.

Staff members may use their phones during school social times but not in front of students. Work phones can be used if it is part of their daily duties. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Staff will be issued with a school phone where contact with students, parents or carers is required. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team. Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose. If a member of staff breaches the school policy then disciplinary action may be taken. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Useful links for students, parents and carers

ChildLine provides free, confidential advice to children and young people 24 hours a day.

Children and young people can talk to a counsellor about how they are feeling by calling 0800 11 11 or by visiting www.childline.org.ukwhere they can have a private one-to-one chat with someone from the children's charity the NSPCC.

Safe search kids.com – This website link will give you some really good advice on how to stay safe online and gives you access to Googles safe search engine for Children.

www.childnet-int.org – A non-profit making organisation working directly with children, parents and teachers to ensure that the issues of online child protection and children's safe and positive use of the Internet are addressed. Childnet International produce an online CD guide specifically for parents KnowITAll – www.childnet-int.org/kia/

www.thinkuknow.co.uk – The Child Exploitation and Online Protection (CEOP) Centre has set up its own edcational website which has been designed and written specifically for children, young people, teachers, parents and carers.

www.getsafeonline.org – A beginners guide to using the Internet safety, including a quiz and some video tutorials about how to 'stay safe' on-line.

www.bullying.co.uk – One in five young people have experienced bullying by text message or via email. This web site gives advice for children and parents on bullying.

www.chatdanger.com – This website is about the potential dangers with interactive services online like chat, IM, online games, email and on mobiles. It provides information, advice, true stories and games. The resource page also contains a number of links to other useful websites.

www.kidsmart.org.uk – Kidsmart is an award winning Internet safety website for parents and those working with children. It has been developed by the children's Internet charity Childnet International and has excellent information on many of the technologies used by children, with guidance on how to 'stay safe' online.

http://www.childnet.com/parents-and-carers – a non-profit organisation working with others to help make the internet a great and safe place for children.

http://www.theparentzone.co.uk/parent – We support parents by working with the practitioners they rely on. From training foster carers on new tech to helping schools develop online safety solutions, we give professionals the skills and information they need to make the internet work for families. We also support families through collaborations with major tech companies and other industry partners.

NSPCC – A Parents Guide to Being Share Aware – A link to a very helpful booklet about cyberbullying from the NSPCC.

NSPCC – NetAware – Find out more about the Apps that children are using and how they are rated and revied by children and parents.

Digital Safety – Some useful tips for increasing your safety online.