www.emmausfederation.co.uk

Federation Internet Access Policy

Creating a safe ICT learning and teaching environment must include effective policies and procedures which are clearly understood and followed by the whole Federation. Acceptable Use Policies are key documents, explaining the ways in which ICT and all the related technologies should be accessed and used by all members of the Federation. They are regularly monitored, reviewed and discussed.
The purpose of Acceptable Use Policies is to clearly set out for the whole Federation:

- the steps taken to ensure the safety of pupils when using the Internet, email and related technologies
- the steps taken by Ark to ensure users have effective and appropriate web filtering when accessing the internet from either school site
- the federation expectations for the behaviour of staff, children and other users whilst using the Internet, email and related technologies within and beyond school
- the federation expectations for the behaviour of staff when accessing and using data
- the federation expectations of parents/carers and the wider community with promoting and supporting the safe and responsible use of ICT and related technologies
- how the federation ensures that pupils, parents/carers, staff, governors and others understand the educational and social benefits that technology can bring to all users, together with being aware of the risks and knowing how to 'Stay Safe' at school, at home and elsewhere.

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children and adults. Consequently, we need to build in the use of these technologies in order to arm our pupils 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
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, Wikis and Podcasting
- Video Broadcasting
- Music and gaming Downloads
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies. At our federation, we understand the responsibility to educate 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 classroom. Schools hold personal data on learners, staff and other people to help them conduct their day to day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.
Everybody in our federation 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.
This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, PDAs, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the federation at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.
ICT authorised staff 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 its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain federation business-related information; to confirm or investigate compliance with federation 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.
ICT authorised staff may, without prior notice, access e-mail or voice-mail accounts where applicable, of someone who is absent in order to deal with business-related issues on that account. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff 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 federation ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

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 head of school or the federation principal. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the head of school.

Acceptable Use Agreement: Pupils

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with others is responsible, polite and sensible.
- I will not deliberately 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 details such as my name, phone number or home address. I will not arrange to meet someone 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 deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, internet and mobile devices are 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. Concerns or clarification may be discussed with the ICT leader.

 I will only use the school's email, internet, intranet, learning platform and any related technologies, including laptops, for professional purposes or for uses deemed 'reasonable' by the Executive 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 pupils, parents and staff are compatible with my professional role.

 I will not give my personal details, such as mobile number/personal e-mail address, to pupils.

 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 used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data may only be taken out of school or accessed remotely when authorised by the head of School, Executive Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.

 I will not install any hardware or software without permission of the Head of School or Executive Headteacher.

 I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

 Images of pupils/staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member. Images will not be distributed outside the school network without permission of the parent/carer, member of staff or Executive 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 the Executive Headteacher. I will check all presentations before I use them with pupils.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

- I will respect copyright and intellectual property rights.

- I will ensure my online activity outside school, will not bring my professional role into disrepute. This includes using sites such as Facebook, twitter and any other social media networks to discuss any school or federation matters.

- I will ensure any social networking within school does not bring my professional role into disrepute. This includes only using sites such as Twitter and any other social media networks to share and promote federation news and diary information.

- I will support and promote the federation e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

February 2018

Review date: February 2020