Foxton Primary School

Acceptable use of ICT Policy

Date:	January 2018
Reviewed by:	
Next Review date:	January 2020
Signed:	

A: Use of school based equipment and services

Access to school equipment, the school network and the internet

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any breach of security to the e-safety coordinator.

- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ headteacher. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety coordinator.

- I will seek consent from the e-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.

- I understand that my files, communications and internet activity may be monitored.

Creation, storage and security of digital content

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption / password protection.

- I will use only school-provided portable storage (USB sticks, SD cards, portable hard drives etc) unless permission has been granted by the e-safety coordinator / headteacher.

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school. I will model safe and responsible behaviour in the creation and publishing of online content.

- I will use only school equipment to create digital images, video and sound unless prior permission is granted by the e-safety coordinator / headteacher.

- I will ensure that I am familiar with the current permission status of pupils (see Parental Consent Form for Digital Images and Video). A summary of all permissions are tabulated and are displayed in the staffroom and accessible in classrooms for reference. If additional permission is needed, e.g. for a surname in the press or for a medical form on SIMS, then I will discuss this with the e-safety coordinator and further written permission will be sought.

- I will ensure that I am familiar with the current Data Protection Policy. I will manage my digital files in accordance with this and I will make myself familiar with procedures in case of a breach of data security.

School email and calendars

- I will use my school email address for all school-related correspondence. I understand that any use of the school email system will be monitored and checked. I will not use my private email account for any school-related business. Email is the main method of communication for all school matters and I will check my e-mail regularly and respond in a timely manner (in normal working hours) to communications that require my attention.

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.

- Communication between staff or members of the wider school community should be professional and related to school matters only. Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect members of staff. All communications to parents and carers should be sent to the office email account for onward transmission. For those members of staff with access to the office account, it is best practice when emailing parents and/or carers to add all intended recipients to the BCC address field. This ensures that parents' personal email addresses are not visible to others.

- To avoid the misrepresentation of others I will not make changes to someone else's e-mail and then pass it on without making it clear where changes have been made.

- The school calendar on Outlook is the central calendar for all school matters. I will check it regularly and take events into account when planning lessons and visits etc. I will add events and appointments to the calendar as necessary. I will also regularly check the school website calendar.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach an age-appropriate e-safety curriculum.

- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour to pupils when using ICT to support learning and teaching.

- I will ensure that I am aware of my 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.

- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

- I will ensure that all online services and software that I use as part of my teaching are appropriate and are used in line with current guidance.

B: Personal equipment and services

Social media and messaging

- I will not talk about my professional role in any capacity when using personal social media. I will not use social media tools to communicate with current or former pupils under the age of 18 nor to communicate with parents in a professional capacity. I will be mindful of potential conflicts of interest where a parent or carer of a child at the school is also a personal friend. I will set and maintain my profile on social networking sites to maximum privacy. I will not access social networking sites for personal use during school hours.

- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and bring this to the attention of the e-safety coordinator or headteacher.

Personal mobile phones and other devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to silent mode during teaching hours and used only in emergencies.

- I will not contact any parents or pupils on my personally-owned device unless in an emergency. If a pupil or parent contacts me using my personal device I will inform the headteacher as soon as possible. On educational visits my personal mobile phone may be used to contact the school.

- I will not use any personally-owned mobile device to take images, video or sound recordings in school.

- I will seek permission from the e-safety coordinator / headteacher if I need to synchronise any school email account with a personally-owned device. If permission is granted then I will ensure that the device has the appropriate technical controls such as encryption / password protection.

Appendix 1 – From EPM's Code of Conduct (ICT and e-safety section)

1.1. Posting, creating, accessing, transmitting, downloading, uploading or storing any of the following material (unless it is part of an authorised investigation) is likely to amount to gross misconduct and result (where the adult is employed) in summary dismissal (this list is not exhaustive):

a) pseudo-images of children (child abuse images), pornographic or sexually suggestive material or images of children or Adults which may be construed as such in the circumstances (that is, writing, texting, pictures, films and video clips of a sexually explicit or arousing nature),

b) any other type of offensive, obscene or discriminatory material, criminal material or material which is liable to cause distress or embarrassment to Foxton School or others.

1.2. If indecent images of children are discovered at the premises or on the equipment/devices, an immediate referral should be made to the Designated Safeguarding Lead and Head Teacher (unless he or she is implicated) and the external Designated Officer (DO) and, if relevant, the police contacted. The images/equipment should be secured, should not be used by others and should be isolated from the network. There should be no attempt to view, tamper with or delete the images as this could jeopardise any necessary criminal investigation. If the images are of children are known to the school, a referral should also be made to children's social care in accordance with local arrangements.

1.3. The contents of our ICT resources and communications systems are our property. Therefore, adults should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

1.4. We reserve the right to monitor, intercept and review, without prior notification or authorisation from adults. Usage of our IT resources and communications systems, including but not limited to telephone, e-mail, messaging, voicemail, CCTV, internet and social media postings and activities is monitored to ensure that our rules are being complied with and for the following purposes:

a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this Code;

b) to assist in the investigation of alleged wrongful acts; or

c) to comply with any legal obligation.

1.5. Adults consent to monitoring by acknowledgement of this Code and the use of our resources and systems. We may store copies of data or communications for a period of time after they are created, and may delete such copies from time to time without notice. If necessary, information may be handed to the police in connection with a criminal investigation.

1.6. A CCTV system monitors the school 24 hours a day. This data is recorded and may be used as evidence of any alleged wrong doing.

1.7. Cyber-bullying can be experienced by adults as well as pupils. Adults should notify the headteacher or the e-safety coordinator if they are subject to cyber-bullying. The school will endeavour to protect adults and stop any inappropriate conduct.

The content of Appendix 1 will be returned to the Code of Conduct when reviewed.

APPENDIX 2 – Pupils' contract for using computers and going online.

Foxton School

Pupils' Contract for using computers and going online

- I will respect the work of others by not looking at it or deleting it.
- I will ask permission before using memory sticks, CDs and DVDs in school computers.
- I will ask permission to go online.
- I will tell an adult straight away if I find online things that I don't like or if I think that others are behaving inappropriately.
- I will only send messages to people that I know.
- I will use a range of passwords, keep all passwords safe and never share accounts.
- I will send messages that are respectful and that use appropriate language.
- If I receive a message from a person that I don't know I will not open it and report it to an adult.
- I will never give out personal details. This includes my name, the school name, my address, my age or any contact information such as telephone numbers. I will not give out the details of others.
- If I use material that is the work of others in my own work, I will state where I found the information.
- If I need to bring a phone to school, I will pass it to the office for safe keeping.