Falconbrook Primary School

E-Safety Policy

Date	Author	Version	Change reference	Approved
February 2018	S Keshtmand		Updated policy	

Contents Page

Introduction

At Falconbrook we believe that computing is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

Computing 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, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to date technologies in both the Learning Zone and classrooms. Computing is a life skill and should not be taught in isolation.

Computing 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 technology within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

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

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Falconbrook Primary School, we understand the responsibility to educate our 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 context of the classroom.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks' (Becta Safeguarding Children Online Feb 2009)

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Whole school approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction (see appendix 1 for staff acceptable use

agreement).

E-safety in the curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- We provide opportunities within the computing and PSHE curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the computing curriculum.
- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

Managing Internet Access

Children will have supervised access to Internet resources

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be

suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.

- Our internet access is controlled through the LGFL web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the head teacher, computing leader or member of SLT.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

E-mail

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international. We recognise that pupils need to understand how to style an email in relation to their age.

- Pupils are introduced to email as part of the Computing Scheme of Work.
- The school gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.

- Staff must inform a member of SLT if they receive an offensive e-mail.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

Social networking and personal publishing

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- All classes has been issued with an iPod touch to use for school photography, assessment notes, emails, music and educational applications. Staff must only use school equipment to take photographs.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

- Data can only be accessed and used on school computers. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head teacher.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Head teacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

See also Anti-Bullying Policy

Cyberbullying is the use of technology, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on
www.kidscape.org and www.wiredsafety.org

Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking

site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the pupil who they have sent messages to.

Investigating Incidents

All bullying incidents should be recorded and investigated in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident (refer to anti-bullying policy)

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with SLT any issue of safety 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.

Falconbrook Primary School

Appendix 1 - Staff Use of ICT Equipment

Introduction

1. This document is recommended as guidance for Governing Bodies to adopt in relation to appropriate use of email, internet and social networking sites by schools' staff.

2. This guidance is recommended to apply to all staff, whether permanent, temporary or casual workers. Agency workers would also be expected to comply with the terms of use of schools' resources where provided but any concerns arising from alleged misuse would be referred to the agency.

3. It is acknowledged that the use of ICT equipment is beneficial and in some cases essential in order that staff may undertake their duties effectively. Staff need to remember however that ICT equipment and services are the property of the school and provided for the purposes of facilitating and supporting the aims of the school.

4. This guidance cannot lay down rules to cover every possible situation. Instead, it is designed to express the schools' philosophy with regard to Information Communication Technology (ICT) resources and electronic communication and to set out general principles staff should apply when using ICT media and services.

5. Schools should take appropriate steps to ensure all staff are aware of the correct usage of schools' ICT resources. This should be covered in the induction of all new staff and all staff should be regularly reminded thereafter, eg at INSET or team meetings. In particular, where ICT equipment is issued to individual staff, a record must be kept and an agreement signed relating to the terms of the loan as set out below.

6. The guidance recommends no personal use of school equipment or resources. If the Governing Body wishes to exercise discretion to allow limited personal use outside of work time then advice should be sought from the human resources team.

Use of the school's ICT equipment

7. ICT equipment includes but is not restricted to computers, laptops , personal digital equipment (PDAs) and mobile telephones issued by the school to staff or available for staff use in the school.

8. Schools will have an 'acceptable use of ICT policy' which all users of ICT equipment are required to be aware of and comply with. Failure to comply with the school's policy may lead to formal disciplinary action.

9. Equipment is available and/or issued to staff for the better performance of their duties and must not be used for personal purposes. Any equipment provided to staff is intended for staff use only, and staff members are responsible for ensuring that this equipment is not used by any other party whilst in their possession, eg family members or friends.

10. When equipment is loaned to staff a loan agreement must be signed by both parties to record the details of the equipment provided and clarify the terms of the loan and intended use of the equipment. A suitable Equipment Loan Form is available for schools to use for this purpose.

11. Staff are responsible for correct usage, safe keeping and storage of equipment whilst it is in their possession. On no account must any school's ICT equipment be left unattended, eg in a vehicle or public place.

12. Staff are expected to be aware of and comply with the schools' requirements regarding data storage and security, particularly when taking equipment off school premises. For example, laptops must not be used to store confidential information; memory sticks should instead be used to store confidential information, eg pupil plans, when there is a need to transport this between systems, and information should be encrypted and password protected.

Email and Internet use

13. Most schools' staff have access to one or more forms of electronic media and services, eg email, internet. Access to such media is given to staff for the better performance of their duties, eg for research and lesson preparation or to communicate with other professional bodies and services.

14. Email accounts and access are provided to staff for the better performance of their duties and not for personal use. In some circumstances, the Governing Body may exercise

discretion to allow limited, authorised personal use outside of work time. Any such use must be authorised in advance.

15. Staff who are required to use email for the better performance of their duties will be provided with an appropriate email account for this purpose. Schools are advised to use a secure email address to protect their systems from viruses and other threats.

16. Staff should treat email as they would any other written communication they may send on behalf of the school and must ensure that care is taken over the content of their emails. Staff should ensure that all emails they send are courteous, polite and professional.

General Principles

17. a. All staff are reminded that email, both internal and external, is to be used for school business only. Unless explicitly authorised in advance, private use (eg shopping) is prohibited.
b. The content of emails sent from school's email accounts and equipment may be checked.
c. Staff should never send emails which may be perceived as derogatory, defamatory, discriminatory or offensive, or which may have a damaging effect on the reputation and/or integrity of the school or its governors, staff, pupils, parents and other service users.
d. Staff should not use email to engage in any purpose that is illegal or contrary to the school's values, policies or interests.
e. All forms of chain mail are unacceptable.
f. Private email accounts, eg hotmail, must not be accessed from the school's ICT equipment or during work time.

18. The use of emails may be monitored and the Head Teacher or other authorised person has the right to access information held on any staff email account at any time.

19. Misuse of the schools' email systems may result in email accounts being restricted or closed and may result in disciplinary action under the school's disciplinary code.

Internet

20. Access to the internet is provided to staff for the better performance of their duties and not for personal use. In some circumstances, the Governing Body may exercise discretion to allow limited, authorised personal use outside of work time. Any such use must be authorised in advance.

21. There are vast amounts of information available on the internet which staff may access for the purposes of their work, eg research. Care should however always be taken to ensure the credibility of the information before it is used.

22. On no account must staff access prohibited websites. These include but are not restricted to gambling, adult interest, personal shopping, banking and social networking sites or sites which may compromise the safety and security of the system.

23. The school reserves the right to monitor internet use and activities.

24. Misuse of the schools' internet may result in access being restricted or withdrawn and may result in disciplinary action under the schools' disciplinary code.

Internet Social Networking

25. The school recognises that there are a number of social networking sites available on the internet which staff may belong to, eg Facebook, Twitter, Bebo.

26. While the organisation does not wish to discourage employees from accessing such sites on the internet, they must never be accessed during work time, or on equipment belonging to the school. Furthermore, when using such sites in their own time certain standards of conduct must be observed to protect both the schools interests and its staff and pupils from the dangers of inappropriate use. Staff should be aware that information posted, even once deleted, may still be available in web archives.

General Principles

27. a. Social networking sites should never be accessed during working hours or using the school's ICT equipment.
b. Staff should never accept or invite friend requests from pupils.
c. Staff should refrain from accepting friend requests from parents.
d. Staff should ensure they adopt the highest possible levels of security (often called privacy settings) when using social networking sites to prevent pupils accessing their web pages and other information.
e. Staff must not post photographs of the school, school events, other staff (without their prior consent), or pupils on social networking sites.
f. Staff must not post information to social networking sites which is confidential to the school or its governors, staff, pupils, parents and other service users.
g. Staff must not post entries on social networking sites or blogs which may be perceived as derogatory, defamatory, discriminatory or offensive, or which may have a damaging effect on the reputation and/or integrity of the school or its governors, staff, pupils, parents and other service users.

28. Recent Employment Tribunal case law has found that activities (ie comments posted by employees on Facebook about their work) “whatever the belief about the privacy of the communications or otherwise were in the public domain”.

29. Failure to comply with the above may result in disciplinary action under the school’s disciplinary code. In addition, the accepting or inviting friend requests from pupils will be investigated under the school’s child protection procedures.

30. Staff should remain vigilant and immediately report any concerns or potential breaches of the above to the Head Teacher [or other authorised person] within the school.

Appendix 2 – Common types of cyber bullying

1. Text messages — that are threatening or cause discomfort – also included here is “bluejacking” (the sending of anonymous text messages over short distances using “Bluetooth” wireless technology).
2. Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
3. Mobile phone calls — silent calls or abusive messages; or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
4. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
5. Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatrooms.
6. Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat.
7. Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal “own web space” sites.

   The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.