E-Safety Policy
Debden C of E Primary Academy

Reviewed by: Matt Hawley	June	2020
Shared with staff:	June	2020
Shared with Governors:	June	2020
Review date:	June	2022

Introduction

At Debden Primary Academy, we believe that ICT is central to all aspects of learning; for adults and children in both the school and the wider community. We believe that our provision should reflect the rapid developments in technology.

ICT 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 suite and classrooms. ICT is a life skill and should be taught across the curriculum.

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 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 Debden Primary Academy, 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.

The ICT leaders will ensure they are up to date with current guidance and issues through organisations such as Lewisham LEA, Becta, CEOP (Child Exploitation and Online Protection), LGFL advice and Child Net.

They then ensure that the Head teacher; Senior team and Governors are updated as necessary.

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 (see appendices)
- 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. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school(see appendix 1 for staff acceptable use agreement).

E-safety in the curriculum

ICT 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 ICT 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 ICT 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 ICT 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. Search engines such as 'Kiddle' are encouraged.
- 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 Essex 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 an ICT leader, technician or member of SLT.
- It is the responsibility of the school, by delegation to the ICT technician, 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 Computer Science 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.
- Staff are encouraged to review their privacy settings on their own social media pages, to ensure that they maintain an adequate level of privacy.

Managing emerging technologies

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

- Mobile phones are not permitted in school for children, and must not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- All classes have access to ipads for use for school photography, assessment notes, emails, music and educational applications. Photos should be deleted from the devices. once used for their desired purpose.

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 of School.

- 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 of School/ Academy Trust, 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

Cyberbullying is the use of ICT, 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.

There are many types of cyber-bullying, these are listed in Appendix 2.

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

See appendix 7 & 8 for Key Safety Advice for children, parents and carers

Supporting the person being bullied

Support shall be given in line with the behaviour policy…

- 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 behaviour policy)

Working in Partnership with Parents

Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school (see appendix 1).

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website)
- A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use.
- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

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.

Appendix 1 – Acceptable Use Agreement

ICT Acceptable Use Agreement

E-Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email 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 other children and adults is responsible, polite and sensible
- I will not 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/others' details such as name, phone number or home address.
- I will not arrange to meet someone or send my image 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 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 my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough

Debden C of E Primary Academy

High Street, Debden, Saffron Walden, Essex. CB11 3LE

Tel: 01799 540302

admin@debden.essex.sch.uk www.debdenprimary.co.uk

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact your child's class teacher in the first instance.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Thank you for your continued support.

Matthew Hawley

Head of School

✂- -

Parent/ carer signature

We have discussed the ICT Acceptable Use Agreement with .... (child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Debden Primary Academy.

Parent/ Carer Signature ....

Class .... Date ....