Discovery Schools Academy Trust

Danemill Primary School

Only the best is good enough.

e-Safety Policy

Reviewed: September 2017

Ratified:

Author: R Hockley

Introduction

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

This policy sets out the ways in which the school will:

⇒ educate all members of the school community on their rights and responsibilities with the use of technology;

⇒ build both an infrastructure and culture of e-safety;

⇒ work to empower the school community to use the Internet as an essential tool for life -long learning.

The e-safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Scope of policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage e-safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate e-safety behaviour that take place in and out of school.

Roles & Responsibilities

The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school community.

The e-safety Leader will work with the Headteacher and the designated Child Protection Coordinators, to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

Role	Responsibility
Executive Headteacher, Head of School and Senior Leaders	◊ Ensure that all staff receive suitable CPD to carry out their e-safety roles ◊ Create a culture where staff and learners feel able to report incidents ◊ Ensure that there is a progressive e-safety curriculum in place ◊ Ensure that there is a system in place for monitoring e-safety ◊ Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff or pupil ◊ Inform the local authority about any serious e-safety issues ◊ Ensure that the school infrastructure/network is as safe and secure as possible ◊ Ensure that policies and procedures approved within this policy are implemented ◊ Use an audit to annually review e-safety with the school's technical support
e-safety Leader	◊ Log, manage and inform others of e-safety incidents and how they have been resolved where this is appropriate ◊ Lead the establishment and review of e-safety policies and documents ◊ Lead and monitor a progressive e-safety curriculum for pupils ◊ Ensure all staff are aware of the procedures outlined in policies relating to e-safety ◊ Provide and/or broker training and advice for staff ◊ Meet with Senior Leadership Team to regularly discuss incidents and developments ◊ Coordinate work with the school's designated Child Protection Coordinator
Teaching and Support Staff	◊ Participate in any training and awareness raising sessions ◊ Read, understand and sign the Staff AUP ◊ Act in accordance with the AUP and e-safety Policy ◊ Report any suspected misuse or concerns to the e-safety Leader and check this has been recorded ◊ Provide appropriate e-safety learning opportunities as part of a progressive e-safety curriculum and respond ◊ Model the safe use of technology ◊ Monitor ICT activity in lessons, extracurricular and extended school activities ◊ Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	◊ Read and understand the Pupil AUP and the agreed class Internet rules ◊ Participate in e-safety activities, follow the AUP and report concerns for themselves or others ◊ Understand that the e-safety Policy covers actions out of school that are related to their membership of the school

Roles & Responsibilities (cont.)

Discovery Schools Academy Trust

Danemill Primary School
Learning and discovering together

Role	Responsibility
Parents and Carers	◊ Endorse (by signature) the Pupil AUP ◊ Discuss e-safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet ◊ Access the school website in accordance with the relevant school AUP ◊ Keep up to date with issues through newsletters and other opportunities ◊ Inform the Head of School of any e-safety issues that relate to the school ◊ Maintain responsible standards when using social media to discuss school issues
Technical Support Provider	◊ Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack ◊ Ensure users may only access the school network through an enforced password protection policy ◊ Maintain and inform the Senior Leadership Team of issues relating to filtering ◊ Keep up to date with e-safety technical information and update others as relevant ◊ Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-safety Leader for investigation ◊ Ensure monitoring systems are implemented and updated ◊ Ensure all security updates are applied (including anti-virus and Windows) ◊ Sign an extension to the Staff AUP detailing their extra responsibilities
Community Users	◊ Sign and follow the Guest/Staff AUP before being provided with access to school systems ◊ Use the Online Compass tool to review e-safety

Teaching & Learning

Why Internet use is important:

⇒ The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

⇒ Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning:

⇒ The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

⇒ Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

⇒ Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Teaching & Learning (cont.)

Discovery Schools Academy Trust

Danemill Primary School
Learning and discovering together

Pupils will be taught how to evaluate Internet content:

⇒ The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

⇒ Children must be taught age appropriate content regarding to e-safety. As well as this the class teacher must ensure that differentiation is provided so that it supports SEN and vulnerable children.

⇒ Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Education of Pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to e-safety'
School Inspection Handbook - Ofsted 2014

A progressive planned e-safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.
Breadth and progression is ensured through implementation of the Somerset Primary Computing Curriculum for KS1 and 2.

Within this:

⇒ key e-safety messages are reinforced through assemblies, Safer Internet Day (February), anti-bullying week (November) and throughout all lessons

⇒ pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the SWGfL scheme of work.

⇒ pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material

⇒ in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches

⇒ pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information

⇒ pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

⇒ pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology

Education of Pupils (cont.)

Discovery Schools Academy Trust

Danemill Primary School
Learning and discovering together

⇒ pupils will read and understand AUP when then access a school system, which will be shared with parents and carers
⇒ pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'

Education and information for parents, carers and wider school community

The school provides information about e-safety and the ways the Internet and technology is used in school to parents, carers and members of the wider community where appropriate. Parents and carers in particular have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. We support them with this by:

⇒ providing a clear AUP for pupils that is shared with parents
⇒ raising awareness through parental events and activities
⇒ regular newsletters and website updates
⇒ providing and maintaining links to up to date information on the school website

Managing Internet Access

The Internet is an open communication channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people everyday as well as a potential risk to young and vulnerable people.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. The following is in place to ensure this.

Information system security:

⇒ School ICT systems capacity and security will be reviewed regularly.
⇒ Virus protection will be updated regularly.
⇒ Filtering protocols
⇒ Keystroke monitoring software

Managing Internet Access (cont.)

Discovery Schools Academy Trust

Danemill Primary School
Learning and discovering together

Published content and the school web site:

⇒ The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

⇒ The computing coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work:

⇒ Photographs that include pupils will be selected carefully and only where permission has been given

⇒ Pupils' full names will not be used when sharing work or images

⇒ Pupil's work can only be published with the permission of the pupil

Social networking and personal publishing:

⇒ The school will block/filter access to social networking sites for the children.

⇒ Teachers will be able to access Twitter for school purposes.

⇒ Newsgroups will be blocked unless a specific use is approved.

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

⇒ Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

⇒ The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

⇒ If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator who will log in the incidents folder.

⇒ Senior leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

⇒ Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

⇒ Videoconferencing will be appropriately supervised for the pupils' age.

Managing Internet Access (cont.)

Managing emerging technologies

⇒ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

⇒ Mobile phones are not permitted at school or around school. If the parents insist that children bring in mobile phones then they must read and sign the Mobile Phone Policy.

E-mail

⇒ E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

⇒ The forwarding of chain letters is not permitted.

Protecting personal data

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

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g. telling a trusted adult, Online bully box, Childline Phone number 0800 1111. Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.

All incidents of cyberbullying reported to the school will be recorded by the school. The school will follow procedures to investigate incidents or allegations of cyberbullying. The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police. Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.

Cyberbullying (cont.)

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include but are not limited to:

⇒ the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content

⇒ Internet access being suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP

⇒ the parent and carers of pupils being informed

⇒ the police being contacted if a criminal offence is suspected