Policy:	**E-Safety Policy** December 2022	
Status:	Non- Statutory	
Review Date:	Three year review December 2025	

General Policy Statement

Diseworth C of E Primary School takes the safety of all pupils and staff very seriously, and this policy is written in order to keep all people in our school community safe and protected. Information Technology (IT) is central to all aspects of learning and our provision should reflect the rapid developments of technology. This E-Safety Policy recognises and seeks to develop the skills that children and adults need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others. We recognise that E-Safety encompasses all electronic devices and communications, including mobile phones and other devices with a wireless connection.

Currently, technologies used by children in and out 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 technologies.

This E-Safety Policy has been developed by a working group of:

- Headteacher and Senior Leaders
- Computing Lead
- Staff - including teachers, support staff, technical staff
- Governors

Whole school responsibilities for e-safety

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.
Staff are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported.

The Computing Lead, Executive Head teacher, Head of School and Senior Leaders, along with Governors will ensure they are up to date with current guidance and issues through organisations such as Leicestershire LA, KCSIE, NSPCC, ChildNet and CEOP (Child Exploitation and Online Protection).

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, iPads and digital cameras
- publication of pupil information/photographs on the school website and Twitter (regarding parental consent)
- their role in providing e-safety education for children
- procedures in the event of misuse of technology by any member of the school community
- have a clear understanding of e-safety issues and the required actions from e-safety training sessions
- reporting any e-safety issues to the Computing Lead, Executive Head teacher and Head of School, as soon as the issue is detected.
- comply with a highly visible staff Acceptable Use Policy (AUP) which staff must sign each year and abide by each time they use school IT equipment and systems, either in the school or elsewhere

Teaching Staff

- Educate pupils on e-safety through **specific and discrete** e-safety lessons (using ProjectEvolve as a base) and reinforcing this in the day to day use of IT in the classroom

Pupils

- participate in gaining an understanding of e-safety issues and the safe responses from e-safety lessons
- comply with a highly visible student's Acceptable Use Policy (AUP) which pupils must abide by each time they use school IT equipment and systems either in the school or elsewhere
- report any e-safety issue to the teacher, support staff or parent.
- take responsibility for their own actions using the internet and communications technologies

Computing Lead, Executive Head teacher, Head of School and IT Support Team

- ensure that the best technological solutions are in place to ensure e-safety as well as possible, whilst still enabling pupils to use the internet effectively in their learning.
- ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, securing and preserving evidence of any e-safety breach.
- deal with e-safety breaches from reporting through to resolution in conjunction with the SLT team
- work with SLT and governors to create, review and advise on e-safety and acceptable use policies.
- work with outside agencies including the police where appropriate.
- maintain a log of all e-safety issues.
- monitor the technology systems which track student internet use to detect e-safety breaches.
- assist in the resolution of e-safety issues with other members of staff

Teaching and learning

Why is internet use important? Diseworth C of E Primary School recognises the internet and other digital technologies provide a vast opportunity for children and adults to raise educational standards, stimulate awareness, enhance and enrich learning, support the professional work of staff and to enhance the school's management functions. Developing effective practice in internet use for teaching and learning is essential.

Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Pupils use the internet widely outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security. The school internet access will be designed for student use and will include filtering appropriate to the age of pupils. Pupils will be taught about acceptable internet use, along with the unacceptable uses and given clear objectives for internet use.

- internet access will be planned to enrich and extend learning activities *(access levels will be reviewed to reflect the curriculum requirements and societies recommendations)*
- staff should guide pupils in online activities that will support the learning outcomes planned
- pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- pupils will be expected to exercise the values of Diseworth C of E school when working on the internet

Evaluating Internet Content In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

- users must act reasonably
- users must take responsibility for their network use *(for all staff, flouting electronic use policy is regarded as a matter for discipline)*
- servers will be located securely and physical access restricted
- the server operating system will be secured and kept up to date
- virus protection for the whole network will be installed and current
- access by wireless devices must be pro-actively managed
- the security of the school information systems will be pro-actively monitored and reviewed by our IT technicians who react to any reports from Sophos (our anti-virus solution); our SIMS data is backed up remotely by LEAMIS
- personal data sent over the internet should be encrypted or otherwise secured
- unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email
- the IT support team will review system capacity although we do not have any restrictions with using Google drive

Emails

- pupils may only use approved email accounts
- pupils must immediately tell a teacher if they receive offensive email
- pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission

School Website

- the contact details on the website should be the school address, email and telephone number
- staff or pupils' personal information must not be published
- school email addresses should be published carefully, to avoid spam harvesting
- the Head of School will take overall editorial responsibility and ensure that content is accurate and appropriate
- the website should respect intellectual property rights and copyright

Use of Images

- pupils' full names will not be used anywhere on the website or internet collaboration tools, particularly in association with photographs
- written permission from parents or carers will be obtained before images of pupils are electronically published

Social Networking

- the schools will block/filter access to social networking sites
- newsgroups will be blocked unless a specific use is approved
- pupils will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations
- pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school name, email addresses, full names of friends, specific interests and clubs etc.
- pupils should be advised not to place personal photos on any social network space
- they should consider how public the information is and consider using private areas
- advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school
- teachers should be advised not to run social network spaces for student use on a personal basis

Filtering

The school will work with ICTIC Support and Schools Broadband to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the computing lead, Executive Head or Head of School. This task requires both educational and technical experience. The support team from ICTIC will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Mobile phones will not be used during lessons or formal school time and will be kept in secure locations. Staff mobile phones will be kept in locations outside the classroom and pupils' phones will be kept safe in the school safe until the end of the school day. The sending of abusive or inappropriate text messages is forbidden.

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

Internet Access

- the school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications
- all staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school IT resource
- at Key Stage 2, access to the internet will be by adult demonstration and recommendations for specific, approved online materials
- parents will be asked to sign and return a consent form for student access

Internet Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Leicestershire CC can accept liability for the material accessed, or any consequences resulting from internet use. The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

E-Safety Complaints

- complaints of internet misuse will be dealt with by the Executive Head teacher or Head of School
- all pupils will be taught to use the internet safely and about the role of CEOP to monitor and report abuse
- any complaint about staff misuse must be referred to the Executive head teacher or Head of school, unless it is the Executive Headteacher or Head of School where complaints will be sent to the Chair of Governors
- parents and pupils 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 IT, 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

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 IT agreements on behalf of their child on admission to school.

- 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, Twitter)

- 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.

Introducing the Policy

- safety training will be given to all to raise the awareness and importance of safe and responsible internet use
- instruction in responsible and safe use should precede internet access
- all staff will be given the School E-Safety Policy and its application and importance explained
- teaching staff will all have accounts on ProjectEvolve to access teaching resources
- staff should be aware that internet traffic can be monitored
- discretion and professional conduct is essential
- staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues
- parents' attention will be drawn to the school's e-Safety Policy in newsletters and through the website
- internet issues will be handled sensitively, and parents will be advised accordingly

Websites offering additional advice and guidance

Childline http://www.childline.org.uk/

Child Exploitation & Online Protection Centre http://www.ceop.gov.uk/

Childnet https://www.childnet.com/

Grid Club and the Cyber Café http://www.gridclub.com/

Internet Watch Foundation http://www.iwf.org.uk/

NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-wellbeing/

Think U Know website http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com/