Dawpool C.E. (Aided) Primary School

DAWPOOL

E-Safety Policy

Vision Statement

‘The Dawpool community are united in their ambition to create a school which embodies the person, love and work of Jesus Christ: a school which enables Christian values to flourish and where all children may experience the abundant life that Jesus offers.’

‘The Fruit of the Spirit is Love, Joy, Peace, Patience, Kindness, Generosity, Faithfulness, Gentleness and Self-Control’ (Galatians 5: 22-23).

Dawpool C.E (Aided) Primary School
School Lane
Thurstaston
Wirral
CH61 0HH

0151 648 3412
schooloffice@dawpool.wirral.sch.uk
www.dawpool-ce.eschools.co.uk
@DawpoolCofE

Table of Contents

INTRODUCTION

The National Curriculum sets the expectation for children to become digitally literate, being able to use, express themselves and develop their ideas through information and communication technology (ICT) in order to prepare them for the future workplace and as active participants in a digital world. It is also a requirement that children are responsible, competent, confident and creative users of ICT.

E-safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding and awareness for users to enable them to control their online experience.

AIMS OF THE POLICY

The purpose of e-safety policy is to provide staff, pupils, parents, governors and visitors specific guidance on how to use ICT safely, responsibly and efficiently. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the virtual or digital world as would be applied to the school's physical buildings. This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. The e-safety policy should be read in conjunction with the safeguarding and anti-bullying policies and privacy notices.

Internet access is used to support and enhance the learning experience of all the pupils at Dawpool school. Knowing that 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.

CONTEXT AND BACKGROUND

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New Internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside school by children include: Internet, e-mail, instant messaging and online chatrooms. It also includes web-based voice and video calling (e.g. Skype and Facetime). In addition, there is online discussion forums social networking sites and discussion blogs. Also, there is YouTube and podcasting mobile phones with camera and video functionality. There are Smart phones with e-mail, messaging and Internet access. All these give us the opportunity to communicate with masses of people.

DAWPOOL'S WHOLE SCHOOL APPROACH TO SAFE USE OF ICT

Creating a safe ICT learning environment includes three main elements at Dawpool school:

• An effective range of technological tools
• Policies and procedures, with clear roles and responsibilities
• E-safety teaching is embedded into the school curriculum and schemes of work.

ROLES AND RESPONSIBILITIES

E-safety is recognised as an essential aspect of strategic leadership in this school. The Headteacher and ICT subject leader, with the support of Governors, aim to embed safe practices into the culture of the school.

Leadership Team

The Senior Leadership Team (SLT) ensures that the Policy is implemented across the school via the usual school monitoring procedures.

E-safety co-ordinator

The designated e-safety coordinator at Dawpool Primary School is Mr Nick Greenop. The role and responsibilities of the coordinator is overseen by the Head teacher.

The key responsibilities of the e-safety co-ordinator include:

• developing an e-safe culture.
• being the main point of contact on issues relating to e-safety.
• raising awareness and understanding of e-safety issues amongst all stakeholders, including parents and carers.
• embedding e-safety in staff training, continuing professional development and across the curriculum and learning activities.
• monitoring and reporting on e-safety incidents to the senior leadership team.
• keeping up with relevant e-safety legislation.
• liaising with the local authority and other agencies as appropriate.
• reviewing and updating e-safety policies and procedures regularly.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-safety policy.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. All staff members should read the school e-safety policy, and ask for clarification where needed. Class teachers should ensure that pupils are aware of the e-safety rules (See Appendix 1), introducing them at the beginning of each new school year.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school.

Parents

Parents can access the e-safety policy, safeguarding policy, anti-bullying policy and privacy notices via our school website and are reminded of their responsibilities at our "learning Links" meetings at the beginning of the new academic year.

INTERNET USE TO ENHANCE LEARNING

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. Using the Internet for learning is part of the National Computing Curriculum. We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

The school Internet access is 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 CHILDREN HOW TO BE SAFE ONLINE

Pupils will be taught, according to their age, how to manage risks when using the Internet.

In the EYFS children will be taught to:

- recognise that a range of technology is used in places such as homes and schools
- elect and use technology for particular purposes.

In KS1, children will be taught to:

- use technology safely and respectfully, keeping personal information private
- identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies.

In KS2, children will be taught to:

- use technology safely, respectfully and responsibly
- recognise acceptable/unacceptable behaviour
- identify a range of ways to report concerns about content and contact
- acknowledge the source of information and to respect copyright when using Internet material in their own work
- be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

A copy of the school's e-safety objectives for each year group is available on the school's website.

If pupils encounter material they feel is distasteful, uncomfortable or threatening, they should report the address of the site to a member of staff. Pupils will also be taught how to report e- safety incidents outside school by, for instance, reporting to CEOP's website (Child Exploitation and Online Protection) and / or childline.

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law and is in accordance with the e-safety policy. The school's e-safety scheme of work follows the Purple Mash schemes of work.

CYBER BULLYING

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself. At Dawpool we take this very seriously and will act upon any incidents and put sanctions in place which may include excluding pupils from communicating via electronic sources during school time.

REPORTING E-SAFETY INCIDENTS

All e-safety incidents should be reported on 'MyConcern' which is acted upon by the Designated Safeguarding Leads and shared with the schools e-safety co-ordinator.

USE OF SCHOOL-RELATED ICT EQUIPMENT OUT OF SCHOOL

Dawpool Primary School provides access/use of ICT equipment to staff. Staff members will have access to the Internet and a variety of applications to enhance pupils' learning within the classroom. The policies, procedures and information within this document apply to all equipment and any other IT handheld or mobile device used in school.

Users Responsibilities

- Users can password-protect their ICT equipment and keep it private.
- Users must not share photos and videos of children taken in school for learning purposes off the school premises.
- Users should only take pictures and videos of children for learning purposes within the school.
- Users in breach of the responsible use policy (see appendix 1) may be subject to, but not limited to, disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
- Dawpool Primary School is not responsible for the financial or other loss of any personal files that may be deleted from an electronic device.

Lost, Damaged or Stolen equipment

- It is a user's responsibility to keep their ICT equipment safe and secure. If they are lost, stolen, or damaged, the Headteacher must be notified immediately. Teachers may be liable for a replacement if due care has not been taken.

Prohibited uses applicable to school's ICT equipment or personal electronic equipment used in school (not exclusive):

Accessing Inappropriate Materials

- All material on the electronic devices must adhere to the e-safety and Safeguarding Policies.
- Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

Illegal Activities

- Use of the school's Internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Users are not allowed to have music and install apps on their electronic devices that violate copyrights.

- Users must use good judgment when using a camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.

DATA PROTECTION

The school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. Personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation, including GDPR. Please refer to the school's privacy notices.

Teachers are given unique login details to the school's network and they should not be shared with other members of staff. Children will be educated on how to manage their passwords safely.

MANAGING EMAIL

Dawpool uses Purple Mash to teach the children how to use e-mails and blogs safely. The settings for this can be managed by the class teacher or the ICT subject leader. Children will be taught not to reveal details of themselves or others, such as address or telephone number.

THE MANAGEMENT OF WEB SITE CONTENTS

The Headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate. The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

MANAGEMENT OF NEWSGROUPS AND CHAT SITES

Pupils will not be allowed access to public or unregulated chat rooms outside the authorised Purple Mash learning platform.

MANAGEMENT OF NEW AND 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 will not be used by

children during school time. Mobile phones must be submitted to the office first thing in the morning and collected at the end of the day.

MANAGEMENT OF INTERNET ACCCES

At Key Stage 1, access to the Internet will normally be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents will be informed that older pupils will be provided with supervised Internet access for learning purposes.

RISK ASSESSMENT

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Dawpool Primary School cannot accept liability for the material accessed, or any consequences of Internet access.

THE FILTERING OF UNSUITABLE MATERIALS

The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.

- A ‘walled-garden’ or ‘allow list’ provides access only to a list of approved sites. An allow list will inevitably restrict pupils' access to a narrow range of information.

- Dynamic filtering examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.

- Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

- Monitoring records Internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report. It is also possible to remove access automatically after a set number of attempts.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. At Dawpool, filtering is performed through Firewall by the Local Authority.

The Headteacher, in consultation with the school's technician, will ensure that regular checks are made to ensure that the filtering methods in use are appropriate and effective. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the E-safety coordinator.

MONITORING

The School Rules for Responsible ICT Use are shared with pupils at the start of every year and as regularly as necessary. Pupils will also be informed that Internet use will be monitored.

All staff must accept the terms of the e-safety responsible use policy. This forms part of the school handbook which is published and shared annually. All staff including teachers, supply staff, classroom assistants and support staff, will be made aware of the school e-safety policy, responsible use policy, safeguarding policy, anti-bullying policy and privacy notices, and their importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user.

The school technician will ensure that the system has the capacity to take increased traffic caused by Internet use. This policy is to be discussed with staff, agreed by the senior leadership and approved by Governors. It will be reviewed annually.

Appendix 1

School Rules for Responsible ICT Use

Keep safe: Keep SMART

1. I will ask permission before using any ICT equipment (e.g. computers, digital cameras, etc), and only use it when a teacher or another adult is with me.
2. I will only use the school's computers for schoolwork and homework.
3. I will not delete any file and I will not look at other people's files without their permission.
4. I will use the usernames and passwords of other children
5. I will not bring software or USB memory sticks into school without permission
6. I will use the internet responsibly.
7. I will only visit web sites that I am asked to by school staff.
8. I will not use Google image search without being asked to do so by a school staff member. I will not download anything (files, images etc) from the Internet unless given permission.
10. I will not use personal email accounts (e.g. Hotmail) at school.

11. The messages I send or information I upload as part of my school work will always be polite.
12. I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission.
13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell a school staff member
14. I will use official websites to help me understand how to keep safe when using ICT.

E-safety staff responsible use policy

This document covers use of school digital technologies, networks etc both in school and out of school.

Access

- I will obtain the appropriate log on details and passwords from the computing subject leader or school technician
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it
- I will not allow unauthorised individuals to access school ICT systems or resources.

Appropriate Use

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed "reasonable" by the Headteacher and the governing body.

Governing Body.

- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-safety co-ordinator or member of the SLT.

Professional Conduct

- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities
- I will not browse, download or send material in school that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate to the headteacher.

Personal Use

- I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes
- I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area
  I understand that the forwarding of e-mail chain letters, inappropriate "jokes" and similar material is forbidden
- I will not use the school Internet facilities for personal access to public discussion groups or social networking sites.

Email

- I will only use the approved, secure email system for any school business: (currently Gmail).
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and I will return it when I have finished with it.

Teaching and Learning

- I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet.
- I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials.
- I will ensure I am aware of digital safeguarding issues so they are appropriately embedded in my classroom practice.

Photographs and Video

- I will not use personal digital cameras or camera phones for taking images of pupils and storing images at home without permission.
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

Data Protection

- I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
- I will not use pupil data, photographs or video from the school on portable devices (e.g. on a laptop, memory stick or any other removable media) for any other purpose but to support learning or a related school project.
- I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises.
- I will respect the privacy of other users" data, and will never enter the file areas of other staff without their expressed permission.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Copyright

- I will not publish or distribute work that is protected by copyright
- I will encourage pupils to reference online resources and websites when they use them in a report or publication.