



Name of Policy	Acceptable Use of Internet /E-safety Policy
Date last reviewed	November 2023
Date to be reviewed	November 2024
Governor Committee	Standards
Key Member of staff	Headteacher, Online safety lead
Statutory	No

This policy is the amalgamation of previous school policies on the Internet, Acceptable use of the Internet By the whole school community and E-safety. It should be read in conjunction with the school’s policies on Child Protection and Safeguarding, Data Protection, as well as the advice offered by Information Commissioners Office (ICO) and Cambridgeshire County Council.

Duxford Church of England Community Primary School is committed to safeguarding and promoting the welfare of children and young people and requires all staff and volunteers to share this commitment.

Contents

1. Intention of this policy	3
2. The teaching of online safety	3
3. Conditions of use	3
4. Services	5
5. Network security	5
6. Physical security	6
7. Wilful damage	6
8. Media Publications	6
Appendix 1 – Letter to parents regarding photographs in school	7
Appendix 2 – Parental consent form	8
Appendix 3 - Event/trip photograph declaration	11
Appendix 4 – Rules for responsible Internet and Computer Use	12

1. Intentions of this policy

Information technology and internet use is a valuable resource to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. It is an essential element of 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access, and hardware and to ensure that pupils and staff can use the internet safely and responsibly as an integral part of the curriculum. Staff will be given yearly online safety training to ensure the importance of online safety within safeguarding is known. Staff will also receive relevant training and knowledge to teach pupils and access the internet safely. All users are required to follow the conditions laid out in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services. In some instances, a breach could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction of how to safely use such resources. Independent pupil use of the internet or the school's intranet will only be permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored, using the smoothwall filtering system, to ensure that they are being used in a responsible fashion.

2. The teaching of online safety

Online safety is an integral part of safeguarding our pupils. Children from year 1-6 are explicitly taught 1 unit of online safety at the start of each academic year. Teachers then add additional online safety lessons in response to the needs of their class and integrate online safety into regular computing lessons. The school's website provides additional teaching resources for parents to access. The Rules for Responsible Internet and Computer Use (**Appendix 4**) are used as a guide to support children being safe and responsible online. The rules are displayed around the school and are read to the children before using the computers.

3. Conditions of use

3.1 Authorised access and filtering and monitoring of the Internet.

The school's Internet access is filtered to block unsuitable websites by the Cambridgeshire County Council ICT services. Pupils will be required to read and agree to comply by the school rules and Internet use. Staff will use official school email addresses to correspond about school matters and pupils will use the STARZ platform.

The School are uses the agent web filter 'Smoothwall' to monitor access.

Sarah Medley is the filtering and monitoring lead. Suzanne Blackburne-Maze and Lionel Beard receive weekly notifications with information regarding internet usage. All notifications are followed up and logged on CPOMS as an online safety concern for children and for adults on a record log kept by the filtering and monitoring lead.

The online safety lead, Jess Ansell, will complete termly checks to ensure that the filters are working appropriately. Check will be completed using the following website: <https://testfiltering.com> In the event of it not working, this will be reported to the filtering and monitoring lead. Following each termly check, Governors will be reported to about the systems efficiency.

3.2 Personal responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to member of staff responsible.

3.3 Acceptable use

Users are expected to utilize the network systems in a responsible manner. It is not possible to set a complete set of rules about what is and what is not acceptable but the pages on network etiquette and privacy together with unacceptable use provides some guidelines on the matter.

3.4 Network etiquette and privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Privacy – do not reveal any personal information (for example home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Password – do not reveal your password to anyone with the exception of pupils sharing their login details with their parents/carers so they can access the schools Virtual Learning Environment (VLE) - such as STARZ, at home. If you think someone has learned your password then contact member of staff responsible.
- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.

- Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
- Staff or pupils finding unsuitable websites through the school network should report the web address to the member of staff responsible.
- Do not introduce 'pen drives' into the network without having them checked for viruses.
- Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity. All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked by the member of staff responsible.
- It is the responsibility of the user (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the internet or intranet does not occur.

3.5 Unacceptable use

Examples of unacceptable use include but are not limited to the following:

- Users must log in with their own user ID and password, where applicable, and must not share this information with other users with the exception of pupils asked to sharing their login details with their parents/carers so they can access the schools Virtual Learning Environment (VLE) - such as the STARZ, at home. They must also log off after their session has finished.
- Users finding machines logged on under another's username should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (for example images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. The County Council have filters in place to block emails containing language that is or may be deemed to be offensive.
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through video conferencing and web broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data. Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.

- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

3.6 Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval.

4 Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

5 Network security

Users are expected to inform member of staff responsible immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must log in with their own user ID and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

6 Physical security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

7 Wilful damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

8 Media publications

Named images of pupils (for example in photographs, videos, web broadcasting, TV presentations, and web pages) must not be published under any circumstances. Written permission from parents or carers will be obtained at the beginning of the academic year, before photographs of pupils are published in school, on the school website or used for publicity by newspapers, magazines etc. (See Appendix 1 for the standard consent form). Parents/Carers and others attending school events/trips will also be asked to sign a form agreeing that any photos they take will be for their own use and not to put these onto any social media site. (Appendix 2) Pupils' work will only be published (for example photographs, videos, TV presentations, web pages) if parental consent has been given.

Appendix 1 – beginning of school letter for photographs in school

Will be issued on headed paper

Date

Dear parents/carers,

At Duxford CofE Community primary school we are required to keep and process certain information about our pupils in accordance with our legal obligations under the General Data Protection Regulation (GDPR). We need to hold personal information about your child on our computer system and in paper records to help us with their educational needs. We have to process personal data in order for our school to run properly, and to fulfil our official functions as set out in law.

We may, from time to time, be required to share personal information about our pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

We use information about your child in a number of different ways, and we would like your consent for some of the ways we use this personal data. We set these out in more detail in the permission leaflet.

If you are not happy for us to use information in the ways we list below, that's not a problem – we will accommodate your preferences.

Similarly, if you change your mind at any time, you can let us know by emailing office@duxford.cambs.sch.uk or by calling the school on 01223 712108 or just popping in to the school office.

If you have any other questions, please get in touch.

Yours sincerely,

Mrs Suzanne Blackburne-Maze and Miss Sarah Medley

Co- headteachers

Appendix 2 - Parental Consent Form

Pupil	
Name	
Year	
Class	
Parent/Carer	
Name	
Relationship to pupil	
Address	
Phone Number	
Mobile Number	
Email	

Please indicate whether you have given your consent in each case by ticking the box on the right-hand side; and sign and date the form on the last page.

Off site activities	Please Tick
----------------------------	--------------------

I give my child permission to take part in:	
<i>Supervised visits/sports events to local destinations during the school day. (Information letters will be sent in advance)</i>	
<i>Local walks (Information letters will be sent in advance)</i>	
Communication	
I give my permission for the school to use my email address to send:	
<i>weekly newsletters</i>	
<i>letters from class teachers</i>	
<i>Information / reminders about school activities sent from the school office</i>	
Food Activities	
Food activities are part of the curriculum, I give permission for my child to:	
<i>sample all foods</i>	
<i>Sample all foods except the following (please provide list):</i>	

I give my consent for the school to contact the following people in the event of an emergency or illness and for my child to be released to them, if I cannot be contacted:

Person 1	
Name	
Relationship to pupil	
Address	
Contact number	

Person 2	
Name	

Relationship to pupil	
Address	
Contact number	

I confirm that I have sought the permission from the people named above and they agree that Duxford CofE Community Primary School may hold their contact details.

Signature

Use of information and image (including photographs and video recordings)

<i>I give permission for my child's;</i>	Yes	No
<i>Image to be used as part of school wall displays/class activities.</i>		
<i>Image (not named) to be used on the school website.</i>		
<i>Image (not named) to be used in external media, e.g Local newspaper press release, village magazines.</i>		
<i>Image to be included in the School's annual class/whole school photographs.</i>		
<i>Image to be included in the School's annual individual photographs</i>		
<i>Image to be used in the school newsletter.</i>		
<i>Image to be used in printed materials, for example, the school prospectus</i>		
<i>Image to be used on social media, for example Twitter.</i>		

In returning this form, I agree that any photos or other images that I take at school events which include images of children other than my own child(ren) will be for my personal use only and that I will not publish the images on social or other media.

The information in this form will be used throughout your child's time at school. You may withdraw your consent at any time by contacting the school. If we do not receive written consent, we have to assume that no consent has been given.

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our record retention schedule for pupil information sets out how long we keep information about pupils.

Please sign and date the form before returning it to the School Office.

Signed: Date:

Appendix 3 – Event/trip photograph declaration

PHOTOGRAPHY AND VIDEOING OF

Event..... Date:

We have been advised that parents may take photographs or make video recordings of school productions for their own private use without breaching the Data Protection Act. They are, of course, not permitted to take photographs or make video recordings for any kind of commercial purpose. Do not place any photos on social media please. Please sign below to indicate that you comply with these requirements.

Name:	Signature:
Name:	Signature:
Name:	Signature:
Name:	Signature:
Name:	Signature:
Name:	Signature:

Appendix 4 – Rules for Responsible Internet and Computer Use

These rules are to be displayed in all classrooms and referred to when using the internet.

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- 1 I will ask permission before entering any Web site, unless my teacher has already approved that site or its address is stored on the Intranet.
- 2 I will only use the specified search engines as and when directed by my teacher.
- 3 I will not enter Internet chat rooms or leave messages on bulletin boards.
- 4 If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- 5 I will not download and install files or software from the Internet.
- 6 I will never reveal or insert my personal details, and home address or telephone numbers on the web or in dialogue with other Internet users.
- 7 I will only e-mail people I know, or my teacher has approved.
- 8 I will always be polite and use appropriate language when sending e-mails.
- 9 I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- 10 I will not intentionally take copyrighted material from the Internet.

11 I will not look at or delete other people's files.

12 I will only use my own log –in codes or passwords to access the computer network.

13 I will not bring floppy CD Roms or memory sticks into school without permission.

14 I know that the school may check my computer files and may monitor the Internet sites I visit.

15 I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.