

DUNNINGTON CE PRIMARY SCHOOL



E-SAFETY POLICY and ACCEPTABLE USE AGREEMENTS

Date of Policy:	March 2020
Date of Review:	March 2023
Member(s) of staff responsible:	Lucy Jarvis
Governor(s) responsible:	School Improvement Committee
Signature of Chair of Governors:	
Date:	5.3.2020



E-Safety Policy and Acceptable Use Agreements

ICT (Information communication Technology) in the 21st Century is seen as 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. There is a need to build in the use of these technologies into our curriculum in order to arm our young people with the skills to access life-long learning and employment.

E-Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Dunnington Church of England Primary. The term 'E-Safety' is used to encompass the safe use of all online technologies in order to safeguard children and adults from known and potential risks.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones
- Internet communications: e-mail and IM (Instant Messenger)
- Webcams and videoconferencing
- Wireless games consoles

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue will be dealt with quickly and within line with this policy. Teachers 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 immediately. Dunnington CE Primary will develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.



E-Safety Policy and Acceptable Use Agreements

Handling E-Safety Complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure. Discussions will be held with the Local Authority Designated Officer for safeguarding and/or a community police officer to establish procedures for handling potentially illegal issues.

This policy aims to inform how pupils and parents/carers are part of the procedures and how children should be educated to make good judgements about what they see, find and use.

Implementation and Compliance

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. In line with the Children's Act 2004 and the government's guidance document 'Keeping Children safe in education', it is the responsibility of schools to ensure that children and young people are protected from potential harm both within the school environment and beyond. It is therefore essential that there is active involvement of both children and their parents/carers for the successful use of online technologies.

Teaching and learning:

Why is Internet use important?

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

The school Internet access is designed expressly for pupil use including appropriate content filtering. Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

As part of the computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.

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

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.



E-Safety Policy and Acceptable Use Agreements

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils;
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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. It is a sad fact that 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 minimise 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.

Roles

Roles: School Leadership

It is the role of the Headteacher and governors to:

- Ensure there is appropriate and up-to-date anti-virus and anti-spyware software on all susceptible devices and that this is reviewed and updated on a regular basis.
- Ensure that filtering is set to the correct level for staff and children.

Roles: e-Safety Leader

It is the role of the designated e-Safety Leader to:

- Provide up-to-date information for all staff to deliver e-safety effectively to pupils.
- Include parents/carers so they feel up-to-date with current government guidance and know where to go for advice.
- Ensure that all adults are aware of the schools filtering levels and why they are in place.
- Record any e-safety incidents to help inform future development and safeguarding.
- Report any e-safety issues to the Headteacher on a regular basis.
- Ensure that the e-Safety policy is reviewed annually.

Roles: Staff or adults at Dunnington Church of England Primary School

It is the responsibility of all staff/adults within the School to:

- Ensure that they know who the Designated Person for Child Protection so that any incidents which involve a child can be reported quickly. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via digital technologies to the Designated Person for Child Protection.
- Be up-to-date with e-Safety information and education that is appropriate for the year group they work with and implant this through their teaching.



E-Safety Policy and Acceptable Use Agreements

- Ensure that all children are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner.
- Ensure that children know what to do in the event of an incident and who to talk to.
- Not disclose security passwords to others.
- Ensure USB drives are encrypted; if any data is required to be taken from the school premises.
- Report any accidental 'misuse' or access to inappropriate materials to the e-Safety Leader.
- The brief use of mobile phones to authenticate email/CPOMs log ins should be restricted to times when pupils are not in the classroom. Other than this, personal equipment such as mobile phones and digital cameras in school for work purposes is prohibited. Any such use should be agreed or reported promptly to the e-Safety Leader or Headteacher.
- Not to store any school personal data such as, pupil levels, pupil photographs or planning with names on it, at home.
- Keep the e-safety Leader up to date with any new issues, procedures and risks that may need to be included within this policy.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff and adults

Roles: Children

Children will be:

- Expected to follow the Acceptable Usage Agreement whilst at school.
- Taught the importance of adopting good e-Safety practice when using digital technologies out of school.
- Taught the need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Roles: Parents/Carers

At Dunnington CE Primary School, we encourage our parents/carers to support the acceptable usage of the internet, within school and also at home. In order to do so, we ask that parents review their child/ children's acceptable use agreement and sign alongside them. We hope that parents/carers will work together with pupils to develop their understanding of the importance of e-safety and encourage regular open conversations to aid this.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Pupils may only use approved internal e-mail software on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- E-mail sent to external organisations should be written carefully and authorised by the class teacher before sending from the teachers email account.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking



E-Safety Policy and Acceptable Use Agreements

- Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others (if allowed home access)
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- The sending of abusive or inappropriate text messages is forbidden.
- On trips staff mobiles are used for emergency only
- Staff should always use the school phone to contact parents, unless in an emergency on a school trip.
- Students and visitors are not permitted to access or use their mobile phones within the classroom. All visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff are only permitted to use their mobile phones to authenticate email log ins briefly at times where pupils are not present. All staff should ensure that their phones are turned off and stored safely at all other times during the teaching day.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- Staff may only use their mobile phones in the staffroom/ school office during the school day (i.e. when children are on the school premises).

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out by Dunlington School.



E-Safety Policy and Acceptable Use Agreements

- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act
- Staff and pupils' personal information will not be published.
- Photographs and videos that include pupils will be selected carefully.
- Pupils' names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".



Growing and learning together and aiming to be the best that we can be, in an environment based on Christian values.'

E-Safety Policy and Acceptable Use Agreements

EYFS Acceptable Usage Agreement



I only go on computers or ipads when an adult has told me it's ok.



I wash my hands before using computers and ipads.



I put ipads back where they belong and don't leave them on the floor.



I only tap or click on things an adult allowed me to use.



I ask before clicking on something new.



I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.

Child Signature _____

Class _____

I understand that the school will monitor my child's use of computers and ipads for their own safety.

Parent Signature _____

Date _____



E-Safety Policy and Acceptable Use Agreements

KS1 Acceptable Usage Agreement



I only access computers or ipads when a trusted adult has given me permission.



I treat computers and ipads with care, washing my hands before use.



I treat ipads with care, never leaving them on the floor and putting them back where they belong.



I understand the importance of turning off a computer correctly every time I am finished with it.



I will tell an adult if a computer is not working correctly or something is damaged.



I only open activities that an adult has told or allowed me to use.



I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.



I know personal information such as my address and birthday should never be shared online.



I know I must never communicate with strangers online.

Child Signature _____

Class _____

I understand that the school will monitor my child's use of computers and ipads for their own safety.

Parent Signature _____

Date _____



E-Safety Policy and Acceptable Use Agreements

KS2 Acceptable Usage Agreement

Staying Safe & Keeping Others Safe

- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will not take or send photos of myself or others online without their agreement and the permission of a trusted adult.
- I will always use my own username and password to access the school network and digital platforms such as Times Table Rockstars.

Acting Responsibly

- I will only use my personal USB stick in school if I have permission to do so.
- I will only access computing equipment when a trusted adult has given me permission.
- I will not deliberately look for, save or send anything that could make others upset.
- I will respect other's work and property and will not change any other person's files or documents.
- I will use all communication tools such as Google chats and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.

T= is it true?

H = is it helpful?

I = is it inspiring?

N = is it necessary?

K= is it kind?

Caring for Computers

- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I understand the importance of turning a computer off correctly every time I have finished using it.
- I agree to report any misuse of computers or iPads or resources, including the internet, to a teacher.
- I will not attempt to install any programmes onto the school machines or alter the computer settings.

In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.



E-Safety Policy and Acceptable Use Agreements

Child Signature _____

Class _____

Parent Signature _____

Date _____

Acceptable usage agreement - all staff in school

User Signature

I have read and understand the policy for E-Safety and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name -----

Signature -----

Date -----

Computer serial number -----

School Policy

This Acceptable Use Policy is intended to ensure

- that you stay safe while using the internet and other communications technologies
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will ensure that you have good access to ICT to enhance your learning and you will agree in return to be a responsible user.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that I act responsibly at all times.

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out here apply to all ICT provided by the school (iPads, netbooks, laptops, email etc) out of school as well as in school
- I understand that the school ICT systems are for educational use and that I will only use the systems for personal or recreational use when I am told it is OK to do so.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.



E-Safety Policy and Acceptable Use Agreements

- I will immediately report any illegal or harmful material or incident I become aware of, to a member of staff
- I will not access, copy, remove or alter any other user's files
- I will communicate with others in a reasonable manner, I will not use aggressive or bad language and I appreciate that others may have different opinions to my own.

- I will ensure that if I take images/videos of others I will only do this if they know about it and have agreed.
- When I use my personal hand held/external devices (iPads/laptops/mobile phones/USB devices etc) in school, I will follow the rules in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will ensure that all files and documents containing pupil details taken offsite on my laptop or on a USB stick are encrypted.
- I will not upload, download or view anything which is illegal or anything which will cause upset to others.
- I will not use any programmes or software that might allow me to bypass the filtering / security systems in place.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school.

I understand that if do not follow this Acceptable Use Policy Agreement, I could be subject to sanctions which could include exclusion from school and the involvement of the police.