

**Norton Canes Primary Academy**

**E-Safety Policy**

|  |
| --- |
| **Date Completed: January 2019****Completed by: Gerry Crofts****Review Date: January 2021** |
|  |

**Norton Canes E-Safety and Acceptable Use Policy**

E-Safety encompasses internet technologies and electronic communications such as mobile phones, iPads and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid. Robust policies and procedures, clear roles and responsibilities, a comprehensive e-safety education programme for pupils, staff and parents and an effective range of technological tools to support e-safety are essential to providing a safe ICT learning environment.

# Context

*“The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.*

*To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom.”* DfES, eStrategy 2005

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

* The Internet
* E-mail
* Instant messaging / video messaging (e.g. Skype) using simple web cams
* Blogs (an on-line interactive diary)
* Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
* Social networking sites
* Video broadcasting sites ( [www.youtube.co](http://www.youtube.com/)m)
* Chat Rooms
* Gaming Sites ([www.minecraft.com](http://www.minecraft.com))
* Music download sites
* Smart phones with camera and video functionality
* Smart phones with e-mail, web functionality and cut down ‘Office’ applications.
* Tablets and iPads.
* Apps (such as Whatsapp and Kik)

***At Norton Canes Primary Academy,*** we apply the Chris Quigley milestones to our curriculum and we use a range of programs such as J2E to enable that children should apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts and that they become independent and discerning users of technology, recognising opportunities and risks and using strategies to stay safe.

# The two E-Safety outcomes for KS1 and KS2 are:

* 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 (KS1)
* Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact (KS2)

Please see the Computing National Curriculum for a further break down of these outcomes.

# Policies and Procedures

* The school’s e-Safety policy will operate in conjunction with other policies including: Behaviour, Anti-Bullying, and Safeguarding.
* The e-Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.
* All Norton Canes, staff and pupils are asked to sign an Acceptable Use Policy (AUP- **see Appendix**) detailing the ways staff, pupils and all network users should use our ICT facilities and reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.
* e-Safety will form a key part of the Computing/PSHE curriculum. Children will be made aware of the dangers and risks of using the internet and mobile technologies throughout the school year. This will form an integral part of computing lessons.

## Internet Access

* 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.
* Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
* The school’s Internet access is designed for pupil use and uses the Staffordshire County Council filtering system.
* Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use. Pupils will not use the Internet without having permission from a member of staff.
* Pupils will not use social networking sites (these are blocked) in school and will be educated about their safe usage in their own time.
* Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
* Pupils are forbidden from downloading games or other programmes from the Internet. Furthermore, such actions are restricted by the school’s internal administrator.
* Downloading programs from the Internet will be carried out by the IT Technician or ICT Leader.
* Public chat-rooms and instant messaging are not allowed and are blocked using the school’s and Staffordshire’s internet filter.
* Access to peer-to-peer networks is forbidden in school.
* Pupils will be educated in ‘Information Literacy’ and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
* The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.
* Pupils will be taught how to report unpleasant Internet content.

## E-mail

* Emails 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.
* Staff should never use personal email addresses to communicate with pupils or parents. An official school email address will be provided by the ICT Subject Leader/administrator.

## Published content and the school website

* Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
* The Deputy Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
* Permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupils’ full names will not be used anywhere on the website or blog, particularly in association with photographs. Additional permission is always sought before publishing photographs for any other use e.g. local media and news coverage. Parents are always advised why the pictures are being taken and how they will be used.
* Work can only be published with the permission of the pupil and parents.
* Pupil image file names will not refer to the pupil by name.
* Pupil image files should be securely stored on the school network.

## Video Conferencing and Webcam Use

* When available, video conferencing and webcam use will be appropriately supervised.
* Pupils (and parents) will be taught the dangers of using webcams outside of school.

## Portable Devices

* Children will not use mobile phones during school time and on school property. For children who walk home alone, phones must to be handed in to the class teacher at the beginning of the day. The sending of abusive or inappropriate text messages is forbidden and children are educated what to do in case this happens.
* Staff should be aware that technologies such as mobile phones can access the internet by bypassing filtering systems and present a new route to undesirable material and communications.
* Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Neither should they use personal cameras to take photographs. Alternative equipment (iPads) will be provided by the school.
* Pupils are taught how to protect themselves from being victims of identity theft and how to report such an event to the correct authority.

# 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.
* Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. These may not be used in school.

# Protecting Personal Data

Everyone responsible for using personal data has to follow strict rules called ‘data protection principles.’ In accordance with the Data Protection Act 2018, they must make sure the information is:

* used fairly, lawfully and transparently
* used for specified, explicit purposes
* used in a way that is adequate, relevant and limited to only what is necessary
* accurate and, where necessary, kept up to date
* kept for no longer than is necessary
* handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction.

# Role and Responsibilities

Our Designated Safeguarding Lead (DSL) is Julie Farmer. Our DSL ensures staff and pupils keep up to date with e-Safety issues and guidance; keeps the senior leaders and governors updated as necessary; ensures that all e-Safety concerns are reported to the necessary agencies/individuals.

Our Governor responsible for Safeguarding is Rachel Frondigoun. Our Governors have an understanding of e-Safety issues and strategies at the school; are aware of local and national guidance on e-Safety; are updated at least annually on policy developments.

Our staff responsibilities are to be familiar with the policy and to adhere to its procedures. They should be familiar with the school’s policy in regard to:

* Safe use of e-mail.
* Safe use of Internet.
* Safe use of school network, equipment and data.
* Safe use of digital images and digital technologies, such as mobile phones, digital cameras and iPads.
* Publication of pupil information/photographs and use of website.
* e-Bullying / Cyberbullying procedures.
* Their role in providing e-Safety education for pupils.
* Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
* Staff will always use a child friendly, safe search engine when accessing the internet with pupils (e.g. Google Safe Search – default settings).
* Staff are to be updated about e-Safety matters at least once a year. At the start of each year, e-Safety will form part of the staff inset.

# Managing Internet Access and Other Technologies

Information system security

* School ICT systems capacity and security will be reviewed regularly.
* All staff and pupils possess individual logons and passwords to the school network with appropriate access rights and privileges.
* Virus protection will be installed on all school computers and updated regularly in light of new viruses and Trojan Horses that weaken the schools security.
* All new software must be installed by the specialist ICT administrator to ensure its safety.

# Managing filtering

* If staff or pupils discover an unsuitable site, it must be reported to the DSL. The website should be minimised to allow for further investigation.
* The IT Administrator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

# Assessing risks

* The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
* The school will give responsibility to the School Business Manager to monitor the use of Internet.
* The school should audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

# Handling e-Safety complaints

* Complaints of Internet misuse will be dealt with by the DSL (Julie Farmer).
* Any complaint about staff misuse must also be referred to the DSL or Assistant DSL (Joe Butler).
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (See Safeguarding Policy)
* Pupils and parents will be informed of the possible consequences for pupils misusing the Internet.
* Pupils and parents will be informed of the complaints procedure.
* Discussions will be held with the police to establish procedures for handling potentially illegal issues.

# Enlisting parents’ support

* Parents’ attention will be drawn to the school e-Safety Policy in newsletters, the school brochure and on the school website.
* Parents will be given a copy of the Acceptable Use Policy that their child has signed. They will be strongly encouraged and supported to monitor their children’s use of technology at home.
* The school will provide regular e-Safety sessions for parents.

# Glossary

**Acceptable Use Policy:** A policy that a user must agree to abide by in order to gain access to anetwork or the internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

**Avatar:** A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

**Chat-room:** An area on the internet or other computer network where users can communicate in realtime, often about a specific topic.

**Filtering:** A method used to prevent or block users' access to unsuitable material on the internet.

**Information Literacy**: The ability to locate pertinent information, evaluate its reliability, analyse andsynthesise it to construct personal meaning and apply it to informed decision making.

**Instant messaging(IM):** A type of communications service that enables you to create a kind ofprivate chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

**Peer-to-peer (P2P):** A peer-to-peer network allows other users to directly access files and folderson each others computer. File sharing networks such as ‘Lime Wire’ create weaknesses in networks security by allowing outside users access to the schools resources.

**Spam:** Unsolicited junk email. The term is also used to describe junk text messages received viamobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

**Spoofing:** Assuming the identity of someone else, using an email address either guessed or harvestedfrom repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

**Trojan Horses:** A virus which infects a computer by masquerading as a normal program. The programcontains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

**Video Conferencing:** The process of conducting a conference between two or more participants over anetwork, involving audio and often text as well as video.

**Virus:** A computer program which enters a computer, often via email, and carries out a malicious act.A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

**Webcam:** A webcam is a camera connected to a computer that is connected to the internet. A livepicture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

# Appendix

* SAFE Use of Internet Poster
* Pupil Agreement



The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

* I will only access the system with my own login and password, which I will keep secret.
* I will not access other people's files.
* I will only use the computers for school work and homework.
* I will not download and use material or copy and paste content which is copyright. (Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the Internet.)
* I will not bring in memory sticks or disks from outside school unless I have been given permission.
* I will ask permission from a member of staff before using the Internet.
* The messages I send will be polite and responsible.
* I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
* I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.
* I understand that the school may check my computer files and may monitor the Internet sites I visit.

