

Northway Primary School



E-Safety Policy 2020-2021

This e-Safety policy has been developed by a working group made up of:

- School Computing Coordinator
- Headteacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors

Scope of the Policy

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place inside and outside of school.

Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

1) Policies and practices

The e-Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the school's approach to E-Safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to E-safety. The code of conduct forms the basis of the schools expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

2) Education and training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an E-safety / computing curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current.

3) Standards and inspection

The school reviews its approach to E-safety on a regular basis to evaluate and improve its provision.

4) Policy Statements

The school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised. As part of the E-safety policy and the acceptable use policy the school will also manage:

- The use of digital images and video
- Data protection
- Digital communications
- Incidents of misuse

The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should never be used for such purposes.
- Care will be taken when capturing digital images and video that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images and videos published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Security and Protection Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All school staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, e.g. no personal data will be stored on USB/memory sticks as these are easily lost.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated. When using communication technologies, the school ensures the following good practice:

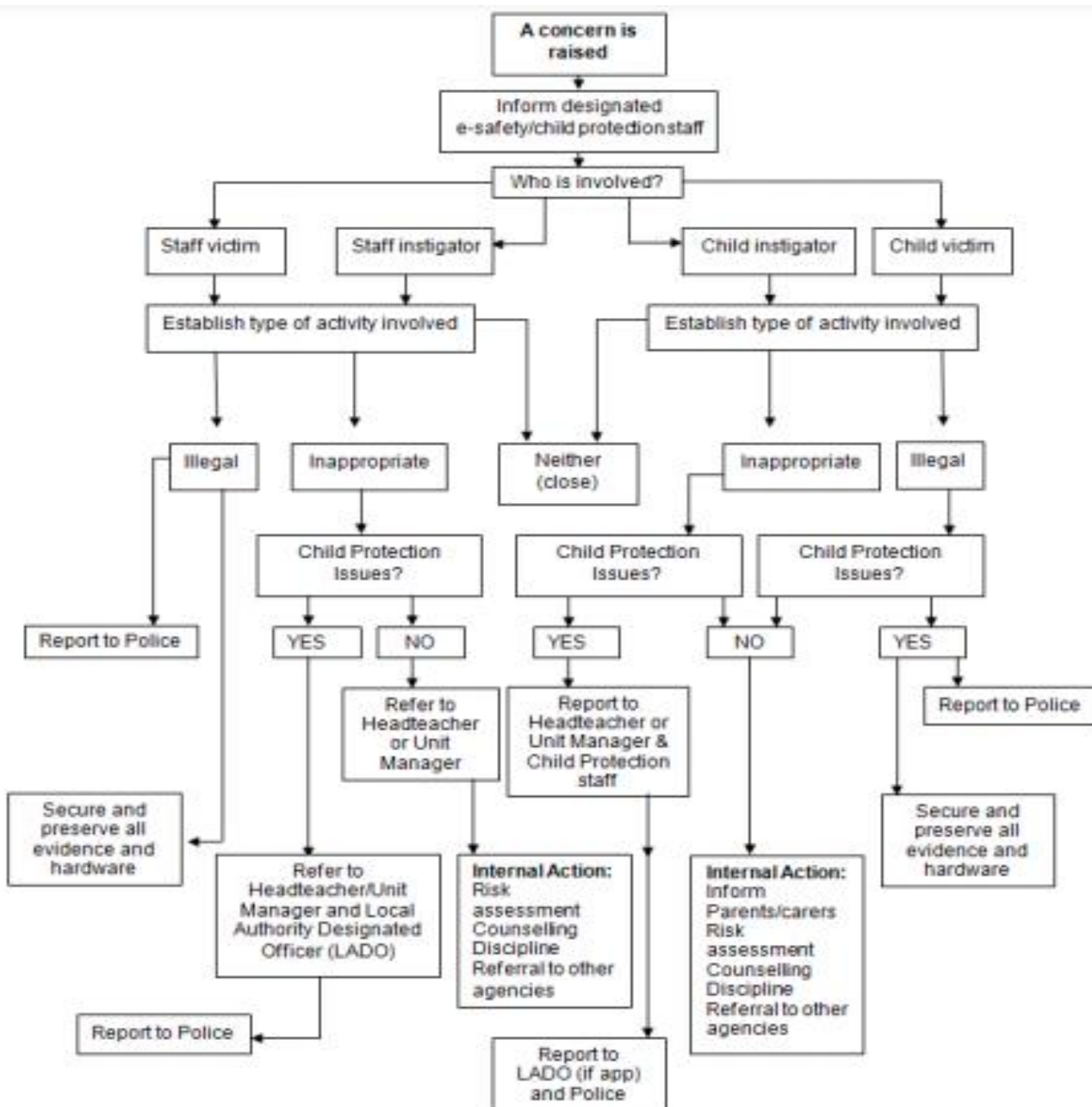
- The official school email service is regarded as safe and secure. Staff should therefore use only the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat/social networking programmes should not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. Computing consultants will be used to monitor misuse and report to e safety officers
- Personal information will not be posted on the school website.

Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work-related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported to the police and could lead to criminal prosecution.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidentally, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below



All incidents will be recorded and reported to the relevant parties and organisations.

Rules for Responsible ICT use for KS1



Think before you

S



I will only use the Internet and email with an adult

A



I will only click on icons and links when I know they are safe

F



I will only send friendly and polite messages

E



If I see something I don't like on a screen, I will always tell an adult

Rules for Responsible ICT use for KS2

Keeping safe: Stop, Think, before you click!

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my classes/ personal workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it and have permission to do so.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.