E-Safety Policy

Northgate Primary School

Approved by:	**Date:** November 2024
Last reviewed on: **December 2025**	
Next review due by: **December 2026**	

This policy should be read alongside:

- *Acceptable Use Policy (AUP) for Staff and Pupils*

All staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Northgate Primary School online safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (completed at staff induction);
- they report any suspected misuse or problems to the Head Teacher / Senior Leader / Computing Leader for investigation and action;
- all digital communications with pupils / parents and carers should be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all relevant aspects of the curriculum and other activities;
- pupils understand and follow the Acceptable Use Policy;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices (i-pads, laptops), cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues.

Parents and carers will be encouraged to support Northgate Primary School in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- Use of communication systems such as tapestry and class dojo
- Monitoring their child's mobile phone according to the home/school agreement

Curriculum:

The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, email, blogging and mobile learning. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems. Whilst internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.

The internet is an essential part of everyday 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.

Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

Education: pupils

Pupils will be educated to take a responsible approach. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Staff should reinforce online safety messages across the curriculum.

- A planned online safety curriculum should be provided as part of Computing lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of class activities.

- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education: parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Newsletters – these will be sent out digitally (via email addresses stored in the school's information management system)
- The online safety section on the school's website
- Parent evenings and information sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to relevant web sites and publications, e.g. www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education and Training: staff and volunteers

It is essential that all staff receive online safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training which will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements.

- The Computing Leader will receive regular updates through attendance at external training events (e.g. from 360 degrees / CAS / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff through email or other communication as appropriate.
- The Computing Leader (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical: infrastructure / equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor (JSPC) but it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of Northgate Primary School's Online Safety Policy and Acceptable Use Agreements. The school should also check their Local Authority policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher through contact with JSPC.
- Licencing of Microsoft is completed through use of an FTE.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for groups of users, for example staff and pupils.

- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person whilst using the school's hardware, mobile technology or the use of the internet.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.

Supply teacher and student logins are available; they use the class laptop whilst in school.

Long term supply and student teachers sign the staff internet Acceptable Use Policy.

Technology:

The technologies to help form a safe environment to learn and work include:

Internet filtering – SurfProtect provided by exa-networks through our managed service provider, JSPC
Antivirus Software – Eset regularly updated and provided through JSPC
Monitoring of pupil/staff activity - Smoothwall