ICT AND INTERNET SAFETY POLICY

Reviewed and updated autumn 2024 | Next review autumn 2025

Introduction

Please read this policy in conjunction with the following policies:

- Child Protection and Safeguarding Policy
- Radicalisation and Extremism Policy
- Anti-Bullying Policy

Background and Rationale

New technologies have become integral to the lives of children and young people, both within Schools and in their lives outside School. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. At home, technology is changing the way children live and activities in which they choose to partake. These trends are set to continue.

While developing technology brings many opportunities, it also brings risks to users and potential dangers of which these are just a few:

- 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 users make contact on the Internet
- The risk of encountering extremist material posted with the aim of radicalising individuals
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying/ sexting and banter / peer on peer abuse
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- 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.

Concerns around internet safety can be categorised into 4 areas of risk; Content, Contact, Conduct, Commerce.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other School policies (e.g. Behaviour, Anti-bullying and Child Protection policies).

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through

good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

The E-safety policy that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents / carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal, and recreational use.

Scope of this Policy

This policy applies to all members of the school community who have access to and are users of 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 are 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 out of School.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

1. Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

2. The Headmistress

The Headmistress is responsible for:

- ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to the Head of IT
- ensuring that the Head of IT and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- serious breaches of protocol by pupils misusing / abusing ICT.

3. The IT Manager

The IT Manager is responsible for:

- the development and maintenance of the ICT network
- ensuring that St Nicholas's ICT infrastructure and data are secure and not open to misuse or malicious attack
- ensuring that users may only access the network through the use of a password.

4. The E-safety committee

The E-safety committee will:

- meet regularly to discuss current e-safety issues.
- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents.
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff.
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- report regularly to Leadership Team.

5. Classroom-based staff

Classroom-based staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels
- they promote e-safety in connection with any curricular work which may involve the use of ICT
- they have an up-to-date awareness of e-safety matters and of the school's current e-safety policy and practices.
- they report any suspected misuse or problem to a member of the IT support staff
- they undertake that any digital communications with pupils should be conducted in a fully professional manner and only using official School systems

Personal Safety of Users

The best way to guarantee safe use of the Internet is for pupils to understand the resources available to them on the Internet and also the related risks to which they may be subject. Pupils are taught to search the Internet effectively to avoid coming across inappropriate material. Website filtering software is also used for this purpose.

At the beginning of each academic year, pupils in all years are taught in ICT lessons about E-safety at an age-appropriate level. E-safety is embedded in the ICT curriculum throughout the school year.

In the interests of all users' personal safety:

- The filtering of internet content provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context.
- The IT Manager and the Designated Safeguarding Lead, are responsible for the filtering of content.
- The School will monitor all use of the ICT systems and other digital resources.
- Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private.
- Users may only access the system with their own secret login name and password.
- They must not attempt to log in to anyone else's account or seek to access their files, this includes staff logging into students accounts.
- Members of staff should not change pupils passwords without their knowledge.
- Pupils need to be aware of the dangers of communicating digital images of themselves or others or posting such images on internet sites.
- If a user forgets their password the person should inform their form teacher who can change it for them.

- Users must not visit sites, make, post, download, upload, data transfer, communicate or pass on any material, remarks, proposals or comments that contain or relate to items that are illegal, defamatory, pornographic or otherwise offensive. Examples of offensive material include, but are not limited to:
    - Child sexual abuse images (illegal – The Protection of Children Act 1978)
    - Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
    - Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
    - Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
    - Sexting/youth produced sexual imagery
    - Upskirting
    - Pornography
    - Promotion of any kind of discrimination
    - Promotion of racial or religious hatred
    - Promotion of terrorism
    - Threatening behaviour, including promotion of physical violence or mental harm
    - Sharing of sexual images (photos, pictures or drawings) and videos, sexual jokes, comments or taunting either in person or on social networking media
    - Any other information which may be offensive to other members of the St Nicholas' community, or which breaches the integrity of the School's ethos.

Pupils should report to an adult member of staff any material, information or messages that make them feel uncomfortable.

Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Staff need to be aware of those pupils who are being targeted by or exposed to harmful influences from violent extremists via the Internet. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against School policies.
- The School will ensure that adequate filtering and monitoring is in place and will review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents should be dealt with as a breach of the acceptable use policies and the School's behaviour and staff disciplinary procedures should be used as appropriate.
- If there is evidence that the pupil is becoming deeply enmeshed in the extremist narrative, the School will act in accordance with the terms of the Radicalisation and Extremism Policy.
- Employees should report any misuse of the School's ICT systems to the IT Manager and the Headmistress.
- If an Employee has access to the Internet at the School, this should be used for educational purposes only. It will be considered to be an act of gross misconduct if they abuse the use of the Internet by using it excessively for personal matters, or at all for accessing any offensive, obscene, pornographic, sexually explicit, or material that is discriminatory on the basis of age, race, religion or belief, sexual orientation, disability, gender reassignment or sex (this list is not exhaustive).

- As anything written on any social media sites is regarded as being in the public domain, transmission of any material that in any way relates to St Nicholas' School and is considered as any of the following will constitute gross misconduct:
    - Bringing the name of St Nicholas' School into disrepute or anything considered embarrassing to the school;
    - Defamatory;
    - Offensive or obscene;
    - Untrue or malicious;
    - In breach of confidentiality or copyright.

Bring Your Own Devices

The school does not permit pupils to bring their own device to School.

Mobile phones may be brought to School if a pupil travels by bus or on foot, but these must be checked into the school office at the beginning of the school day and collected at the end. Pupils only access to the internet during the school day is therefore through the school computers which have filtering and monitoring systems in place. The guest network is monitored for student devices, if devices are detected the school guess network password is changed.

Transferring work between Schoolwork and home computers

To safeguard the security of our computer network, and also of the user's personal data, the school discourages the use of USB drives. Work can be transferred between School computers and home either via Office 365. Office 365 enables Microsoft software either to be used in the cloud or downloaded onto a home computer for the duration of a pupil's education at St Nicholas' School.

Printing

The school is aware of its responsibility towards the environment and pupils are asked to refrain from unnecessary printing. Work that does need to be printed should be checked carefully before printing to avoid wastage, and permission requested from a teacher before printing out.

To encourage responsible printing behaviour, pupils are assigned a set number of credit each month which can be used to print. These credits do not rollover month to month and the maximum value is reset on the first day of the month. Additional credits can be requested from the IT Department if suitable reason is given.

Senior pupils doing homework on home computers should also print this at home wherever possible. If this is not possible, pupils may then print in the Senior ICT Suite at lunchtimes or during Homework Club, at the teacher's discretion.

Social Networking

The school accepts that pupils are likely to use social networking sites such as Facebook (but not before the age of 13), Twitter, Instagram, Snapchat and WhatsApp as a means of communicating with friends, family and others. Whilst they can be a good way to keep in touch, social networking sites can expose pupils to a variety of risks. These can range from personal difficulties such as distraction from studies and everyday life, loss of self-esteem and falling out with peers to wider issues such as identity theft and grooming. Some of these also risk bringing the school's good name into disrepute.

Our E-safety curriculum for older girls aims to help them to be mindful of the wise use of social networking. This includes making them aware of:

- How to manage privacy settings;
- The longevity of social media postings and photographs;
- The fact that future employers are likely to check their digital footprint;
- The importance therefore of not posting online:
    - confidential or personal information;
    - unpleasant or unkind comments;
    - inappropriate photographs of themselves;
    - photographs of others without their permission.

Parents also have a responsibility to be vigilant as to their child's use of social networking and are encouraged to reinforce the above points. Parents are advised to monitor their child's use of the Internet, to limit it to an agreed time per day, and also to restrict the use of computers, tablets or smartphones in an unsupervised area such as the child's bedroom. Parents should be just as vigilant about smartphones as any other kind of computer. We recommend a "digital sunset": there is no need for your daughter to have her phone in her bedroom at bedtime. We also recommend that parental controls are used to restrict the apps that their child is able to download onto their phones.

Cyber-bullying

Cyber-bullying is the use of the Internet, social networking sites, mobile phones, and other electronic devices to deliberately upset others. It can occur at any time. Perpetrators can remain anonymous.

Cyber-bullying is against the law and the school treats all cyber-bullying very seriously. Cyber- bullying which puts the welfare and good name of the school at risk, which occurs on or off School premises, may be considered gross misconduct and may incur disciplinary action.

Filtering and Monitoring

The school uses Smoothwall for its filtering and monitoring system. Smoothwall is a member of Internet Watch Foundation and signed up to Counter-Terrorism Referral Unit list. The provision of this system will be reviewed by the e-safety committee at least annually, in line with an update of this policy, or as and when an issue is identified.

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or School administration
- restrict students from learning how to assess and manage risk themselves

Decisions about what is appropriate will be made by the e-safety committee and implemented by the IT Network Manager.

The filtering system will apply to all student, staff and guest accounts including all devices using the school broadband connection. The filtering system will;

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings, and abbreviations

- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide email alerts when any web content has been blocked which are checked by the network manager and the DSL.

The filtering systems will allow the school to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

The network manager will run termly checks using Testfiltering.com to check the effectiveness of the system. These will be sent to the DSL and any failings will be addressed immediately.

All staff will be trained on the expectations, applicable roles, and responsibilities in relation to filtering and monitoring during their induction. Regular updates to this will be incorporated into the safeguarding training updates which take place during INSET, in briefings and via email.

All staff are made aware of the reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Cyber Crime

The school will have an appropriate level of security protection in place to safeguard their systems, staff and learners. The e-safety committee will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

All Servers and endpoints have windows defender for antivirus and anti-malware protection. Smoothwall has anti-virus protection for files downloaded from the internet. Microsoft exchange is used for email filtering. Smoothwall also provides intrusion detection system (IDS).

Monitoring Use

The school regularly monitors use of the School's ICT facilities for signs and patterns of abuse via Smoothwall.

In accordance with section 550ZC of the Education Act 1996 and the Department for Education's guidance 'Screening, Searching and Confiscation', the school may examine a pupil's property, including mobile phones or other devices where there is 'good reason' to do so. Good reason includes a reasonable suspicion that the data or file on the device has been, or could be, used to cause abuse, harm, or break the school rules.

Breach of this policy

The use of the system for any inappropriate communication will be dealt with through the school's disciplinary procedure. Serious or persistent disregard for this policy may lead to suspension or expulsion.