NORTH STAR
COMMUNITY TRUST

Technology and online safety

Primary and Secondary Academies

September 2026

Introduction

Information and Communications Technology (ICT) is an essential resource to support learning and teaching both in school and during periods of remote learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, academies now include the use of these technologies in order to arm our young people with the skills to access Information Technology.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Some of the internet content pupils can access both inside and outside of the classroom include but are not limited to: -

- websites
- e-mail, instant messaging and chat rooms
- social media (such as Instagram, Facebook and Twitter)
- online gaming
- learning platforms and virtual learning environments
- blogs and wikis
- podcasts
- video broadcasting
- music downloads
- online meeting platforms (such as Zoom and Microsoft 'Teams')
- A.I. tools

Increasingly pupils have access to a variety of devices enabling online content including: -

- smart phones (with either text, video or internet access)
- tablets, smart watches or other mobile devices with internet access
- games consoles
- smart televisions
- smart speakers and similar devices

Whilst useful both in and out of the context of education, much ICT (particularly web-based resources) are not consistently policed or regulated. All users need to be aware of the range of

risks associated with the use of these internet technologies and that some have minimum age requirements (often 13 years in line with UK GDPR).

Our Academies understand the responsibility to educate our pupils in online safety issues by teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies both in and beyond the context of the classroom.

Internet

Our school has a duty to provide pupils with quality Internet access as it is an essential part of education. The purpose of the internet in a school environment is to help raise educational standards of pupils and allows them to develop the necessary skills for living in a technological society.

Internet use is part of the curriculum and a necessary tool for learning as well as an essential element in 21st century life for education, business and social interaction. Pupils will likely use the Internet outside of the school environment and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The benefits of using the Internet in education include: -

- access to world-wide educational resources (such as museums and art galleries)
- access to appropriate child friendly resources and information
- inclusion in government initiatives
- educational and cultural exchanges between pupils both nationally and world-wide
- cultural, social and leisure use in libraries, clubs and at home
- access to experts in many fields for both pupils and staff allowing access to new and refreshing teaching materials
- enhanced academy communication with advisory / support services, professional associates and colleagues
- exchange of curriculum and administrative data with the Department for Education
- access to learning wherever and whenever required.

Online safety and the curriculum

ICT and online resources are increasingly used across the curriculum, in which online safety is embedded, as it is essential for guidance to be given to the pupils on a regular and meaningful basis.

We teach internet skills in ICT / PSHE lessons, through targeted assemblies and workshops at our academies and provide opportunities within a range of curriculum areas to teach about online safety.

We educate pupils about the online risks that they may encounter outside of the academies and this is done both informally when opportunities arise and as part of the online safety curriculum.

We continually look for new opportunities to promote age appropriate online safety.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk: -

- **Content**

  being exposed to illegal, inappropriate or harmful content (e.g. pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalization, extremism, misinformation, disinformation (including 'fake news'), conspiracy theories and content generated, altered or distributed using artificial intelligence).

- **Contact**

  being subjected to harmful online interaction with other users or generative AI applications that simulate this (e.g.peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes)

- **Conduct**

  online behaviour that increases the likelihood of, or causes, harm (e.g. making / sending / receiving explicit images including those generated using AI, consensual and non-consensual sharing of nudes, semi-nudes and / or pornography, sharing other explicit images) and online bullying (including the creation, alteration or sharing of AI-generated or manipulated images or videos intended to humiliate, bully, intimidate or harm another person)

- **Commerce**

  risks such as online gambling, inappropriate advertising, phishing or financial scams

Our academies will ensure that: -

- internet access levels will be carefully monitored and reviewed to reflect the curriculum requirements and age of pupils. Staff will preview any recommended sites before use.
- internet access will be planned to enrich and extend learning activities.
- staff will guide pupils in on-line activities that will support the learning outcomes planned for pupils' age and maturity.
- staff will model safe and responsible behaviour in their own use of technology during lessons.
- pupils will be educated in taking responsibility for their own safe Internet access
- pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- if Internet research is set for homework, parents may be advised to supervise research.

Pupils are taught to: -

- critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- understand that the Internet safety rules apply to any use of the Internet regardless of which electronic device it is accessed
- develop a range of strategies to evaluate and verify information before accepting its accuracy
- have age appropriate awareness that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- know how to narrow down or refine a search (and for older pupils; to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- have age appropriate awareness of the materials they are shown and how to validate information before accepting its accuracy.
- to understand how photographs can be manipulated (including AI manipulation) and how web content can attract the wrong sort of attention;
- have age appropriate awareness of plagiarism, intellectual property and copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- understand acceptable behaviour when using an online environment / email, i.e. be polite, no

bad or abusive language or other inappropriate behaviour; keeping personal information private;

- understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- understand why they must not post pictures or videos of others without their permission;
- know not to download files (such as music files) without permission;
- have strategies for dealing with receipt of inappropriate materials (and for older pupils to understand why and how some people will 'groom' young people for sexual reasons and / or radicalisation);
- understand the impact of cyberbullying, the making or sharing of nudes and semi-nudes including AI-generated or manipulated intimate images, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
- be aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technology (e.g. parent / carer / teacher / trusted staff member, or organisations such as the London Grid for Learning, Childline or the CEOP 'Report Abuse' mechanism).

Online safety and e-mails / instant messages

- Pupils are taught that they must immediately tell a teacher / trusted adult if they receive an offensive email or instant message through any platform
- Staff must inform their head teacher / line manager (and the safeguarding team where appropriate) if they receive an offensive email or instant message
- Pupils should only use academy approved accounts on the academy system and only for educational purposes.

Remote learning

- Academies will always make sure the platform that they are using is suitable for the children's age group, stage of development and ability.

- Academies will set up school accounts for any online platforms they use. It is never appropriate to use teachers' personal accounts.
- Academies will always double check the privacy settings on online platforms prior to rolling these out to pupils.
- Academies will communicate clearly to parents, carers and children our expectations of them in order to keep pupils safe online and
- Academies will clearly communicate with parents regarding the benefits and risks of online lessons.
- Where academies record or livestream lessons via an online platform, a risk assessment will be completed and appropriate actions will be identified and undertaken to minimise harm.
- We recognise that teaching online is different to teaching face-to-face but expect all adults to always maintain professional relationships with children and young people.
- Academy staff are regularly reminded of our staff code of conduct and are clear on the expectations in terms of behaviour when teaching via online platforms.
- When live streaming lessons (or recording them for future playback), teachers are expected to work in a neutral area where nothing personal or inappropriate can be seen or heard in their background.
- Staff are aware that usual safeguarding expectations apply during online teaching and know how to report any safeguarding concerns through the usual reporting channels.
- Sometimes staff might need to contact children individually, via online platforms for example to give feedback on homework. Staff should only contact children during normal school hours, or at times agreed by the academy's leadership team.
- Staff must always school accounts to communicate via email or online platforms, never teachers' personal accounts.
- Any one-to-one online sessions (for example pastoral care meetings), must be risk approved by the school's leadership team.
- Staff know what safeguarding measures to take if they are having a one-to-one conversation with a child.

Online safety roles and responsibilities

- As online safety is an important aspect of strategic leadership within the school, the Trustees, Chief Executive Officer, Governors and Head teachers have ultimate responsibility to ensure that policies and practices are embedded and monitored.
- As online safety links closely to safeguarding, it is the role of the designated safeguarding leads to keep abreast of current issues and guidance through organisations such as Childnet, CEOP (Child Exploitation and Online Protection) and UKSIC (UK Safer Internet Centre). All members of the academy community are made aware of who holds these posts.
- We will remind students about their responsibilities through an acceptable use statement which they will sign with their parents (See **APPENDIX 1** and **APPENDIX 2**).
- New staff receive information on the school's ICT Code of Conduct and acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- Teaching staff receive regular information and training on online safety and how they can promote the '*stay safe*' online messages.
- All teaching staff are encouraged to incorporate online safety activities and awareness within their curriculum areas. We endeavour to embed online safety messages across the curriculum whenever the internet and / or related technologies are used.
- The topic of online safety will be embedded throughout our teaching.
- The key online safety advice will be promoted widely through our website, newsletters, class activities etc
- Academies will log all incidents in order to monitor what is happening and identify trends or specific concerns.

Misuse and infringements

- Complaints and / or issues relating to online safety should be made to a member of the Senior Leadership Team or the head teacher. Incidents should be logged
- Any form of cyberbullying will be dealt with in line with our behaviour policy
- Parental complaints will be dealt with in line with the complaints procedure.
- All users are aware of the procedures for reporting accidental access to inappropriate

materials. The breach must be immediately reported to a member of the Senior Leadership Team or the head teacher

- Deliberate access to inappropriate materials by any user will lead to the incident being logged as a safeguarding concern. Depending on the seriousness of the offence there may be an investigation by the head teacher or their nominee and police involvement for serious incidents.

Computer viruses

- Pupils and staff using personal removable media are responsible for measures to protect against viruses (e.g. making sure that additional systems used have up-to-date virus protection software). It is not the responsibility of NSCT Academies to install or maintain virus protection on personal systems.

- Neither pupils nor staff are permitted to download programs or files on school based technologies without seeking prior permission from the IT department

Parental involvement

We believe that it is essential for parents / carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety with parents / carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

- Parents / carers and pupils are actively encouraged to contribute to adjustments or reviews of the school online safety policy by contacting the head teacher

- Parents / carers are asked to read through and sign acceptable use agreements with their child on admission to the school. (See **APPENDIX 1** and **APPENDIX 2**)

- The school disseminates information to parents relating to online safety where appropriate in the form of: -

    - information and celebration evenings
    - practical sessions (e.g. how to adjust Facebook privacy settings)
    - posters
    - school website
    - newsletter items

Passwords and password security

Pupils must keep their passwords private and not to share with others, particularly their friends. Both staff and pupils are regularly reminded of the need for password security.

Filtering and monitoring

Our school teaches Online Safety through PSHE, RSE Period 1 form time, assemblies and through many of our timetabled lessons where appropriate. A whole school approach to online safety will protect and educate our pupils in their safe use of technology, as well as allowing staff to identify, intervene and escalate any concerns as appropriate. It is essential that our pupils are safeguarded from potentially harmful and inappropriate material online.

Filtering

Using available technology to restrict user access to potentially harmful content.

Monitoring

Using available technology to detect inappropriate internet use on our network

Whilst appropriate filters and monitoring systems are in place it should not unreasonably restrict what pupils can be taught with regards to online teaching and safeguarding. When children use the school's network to access the internet, they are protected from inappropriate content by these filtering and monitoring systems to the best of our ability.

The Department for Education guidance, 'Keeping Children Safe In Education' states that schools must: -

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually (and record the outcome of the review).
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

The Department for Education guidance, 'Keeping Children Safe in Education' also expects that a review of the effectiveness of filtering and monitoring is carried out at least once every academic year. Reviews should be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. They should include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record should be kept of these checks.

In our schools: -

- the 'monitoring and filtering' lead is the Trust's Head of Safeguarding in collaboration with the school Designated Safeguarding Lead (DSL).
- our Trust Filtering system is provided by LGfL (London Grid for Learning) and is reviewed at least annually by the Trust's Designated Safeguarding Lead's and the IT team.
- our schools use Smoothwall filtering and monitoring system which is designed to prevent access to inappropriate content and notify the DSL team both immediately and in a weekly report.

As a trust, we can adapt this system to meet the needs of our curriculum to ensure continuity to our teaching and learning content, while making sure that all safeguarding concerns are followed up with students and where appropriate parents / carers and external agencies.

Mobile phones and mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies (such as smartphones, iPads, games players) are generally very familiar to pupils outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Please refer to our *Safeguarding, Child Protection and associated procedures* with regard to youth produced sexual images and '*sexting*'.

The latest Keeping Children Safe in Education DfE guidance states that all schools should be mobile phone-free environments by default; anything other than this should be by exception only.

Use of artificial intelligence (AI)

AI (Artificial Intelligence) refers to technology that can create new, 'natural'-seeming content (i.e. it seems like it was created by a person and not a computer) by drawing from large volumes of existing information.

AI cannot provide definitive answers or solutions as any responses or content it returns can differ each time as: -

- it will depend on how questions or inputs are phrased by the user; and
- responses are usually derived from information on the internet which itself may neither be up to date nor reliable.

- it may generate information which is incorrect, biased or inappropriate

We recognise that generative AI can create, alter or manipulate content, including images, audio and video, and that AI-generated or manipulated content may present safeguarding risks, including harmful or inappropriate content, bullying, harassment, exploitation and abuse.

Appropriate use

Where it is age appropriate for them to use it, students should ensure that they label any AI-generated content they have used.

Approval is likely to be permitted for the following types of use: -

- as a research tool
- idea generation for projects
- analysing text to recommend changes / improvements
- generate summaries or explanations of topics or concepts for revision or learning purposes

Inappropriate use

Pupils must **not** use any AI tool for any of the following purposes: -

- generating inappropriate images or other harmful or abusive content
- using any personal details or images of staff or students within an AI model
- using generative AI as a method to humiliate, bully, intimidate or harm anyone else
- copying or paraphrasing sections of AI-generated content so that the work is no longer the pupil's own
- copying or paraphrasing whole responses of AI-generated content
- using AI to complete parts of assessments so that the work does not reflect the pupil's own work, analysis, evaluation or calculations
- failing to acknowledge use of AI tools when they have been used as a source of information
- incomplete or poor acknowledgement of AI tools
- submitting work with intentionally incomplete or misleading references.

Failure to comply with this may result in behaviour related sanctions for pupils

AI-generated or manipulated images or videos of children, including deepfakes, which are sexual or intimate in nature must be treated as a safeguarding concern and managed in accordance with the academy's safeguarding and child protection procedures.

Acceptable use agreement / online safety for **Primary Academy** pupils

Dear Parent / Carer

Information and communications technology (ICT) includes the internet, e-mail, digital videos and mobile technologies. ICT is an important part of learning in our academy and we expect all children to be safe and responsible when using any.

Parents are expected to read and discuss our online safety rules with their child and then to sign and return this agreement. If you have any concerns or would like some further explanation, please contact the academy directly.

If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is always advised that parents recheck these sites and supervise this work or any further research.

I will: -

- only use ICT in school for school purposes
- only log on to the school network, other systems and resources with my own user name and password
- (if I am given one) only use my class / school e-mail address when e-mailing
- be responsible for my behaviour when using the Internet (which includes resources I access and the language I use)
- follow the school's internet safety rules
- ensure that all my ICT contact with other children and adults is responsible, polite and sensible.
- ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- respect the privacy and ownership of others' work on-line at all times.

I will not: -

- tell others my passwords.
- bring any ICT equipment or devices into school without my teacher's permission (this includes mobile phones, i-pods, games, cameras, usb drives and software).
- download or install software on school technologies

- give out personal details (such as my name, phone number or home address) without a teachers permission
- deliberately upload, manipulate (including AI manipulation) or add any images, video, sounds or text that could upset any member of the school community
- deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- use ICT for any other purpose than to complete schoolwork. I understand it is not for personal use.

I understand that: -

- these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent / carer may be contacted.
- online content is filtered and schools are required to monitor pupils internet and web browser use to highlight any safeguarding concerns or online use that is deemed inappropriate. The monitoring also applies to any devices the school has provided.

Declaration for: PRIMARY ACADEMY PUPILS

We have discussed the acceptable use agreement for primary children and my child agrees to follow the online safety rules and to support the safe use of ICT at the Academy.

Academy	Enfield Heights ACADEMY	Kingfisher Hall ACADEMY	Woodpecker Hall ACADEMY
Please tick**: -**	☐	☐	☐

Name of child .....

Parent / carer name .....

Parent / carer signature .....

Child's class ..... Date .....

Acceptable use agreement / online safety for **Secondary Academy** pupils

Dear Parent / Carer

Information and communications technology (ICT) includes the internet, e-mail, digital videos and mobile technologies. ICT is an important part of learning in our academy and we expect all children to be safe and responsible when using any.

Pupils are expected to read and discuss our online safety rules with their parent or carer and then to sign and return this agreement. If you have any concerns or would like some further explanation, please contact the academy directly.

If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is always advised that parents recheck these sites and supervise this work or any further research.

I will: -

- only use ICT in school for school purposes
- only log on to the school network, other systems and resources with my own user name and password
- (if I am given one) only use my class / school e-mail address when e-mailing
- be responsible for my behaviour when using the Internet (which includes resources I access and the language I use)
- follow the school's internet safety rules
- ensure that all my ICT contact with other children and adults is responsible, polite and sensible.
- ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- respect the privacy and ownership of others' work on-line at all times.

I will not: -

- tell others my passwords.
- bring any ICT equipment or devices into school without my teacher's permission (this includes mobile phones, i-pods, games, cameras, usb drives and software).
- download or install software on school technologies

- give out personal details (such as my name, phone number or home address) without a teachers permission
- deliberately upload, manipulate (including AI manipulation) or add any images, video, sounds or text that could upset any member of the school community
- deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- use ICT for any other purpose than to complete schoolwork. I understand it is not for personal use.

I understand that: -

- these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent / carer may be contacted.
- online content is filtered and schools are required to monitor pupils internet and web browser use to highlight any safeguarding concerns or online use that is deemed inappropriate. The monitoring also applies to any devices the school has provided.

Declaration for: SECONDARY ACADEMY PUPILS

We have discussed the acceptable use agreement for secondary students and my son / daughter agrees to follow the online safety rules and to support the safe use of ICT at the Academy.

Academy	Heron Hall ACADEMY

Name of pupil .....

Pupil's signature .....

Parent / carer name .....

Parent / carer signature .....

Pupil's class ..... Date .....