E- Safety Policy

Author	E. Cruse/O Benzie	Source	The Key/National Online Safety
Approved by	Trust Board	Status	Draft
Last review	Sept 2024	Next review	Sept 2026

Details of Policy Updates

Date	Details
March 2020	Addition of 3.4 ICT Lead responsibilities, Addition of 5.6 Curriculum Content, Addition of 5.7 Education of Parents Section, Addition of 11 Training Section
February 2021	Updated establishment name
November 2022	Addition of 9.4 Dealing with incidents
September 2024	Re write in line with National online safety advice
December 2024	Additional appendices regarding acceptable use for visitors – not passed for ratification due to appendices only.
February 2026	Addition of Appendix D – The Use of AI

Contents:

North Star Academy Trust E-Safety Policy

Statement of intent

North Star Academy Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019

- The UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018

- DfE (2023) 'Filtering and monitoring standards for schools and colleges'

- DfE (2021) 'Harmful online challenges and online hoaxes'

- DfE (2023) 'Keeping children safe in education 2024'

- DfE (2023) 'Teaching online safety in school'

- DfE (2022) 'Searching, screening and confiscation'

North Star Academy Trust E-Safety Policy

- DfE (2023) 'Generative artificial intelligence in education'

- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy and Code of Conduct

- Staff code of conduct

- Technology Acceptable Use Agreement

- Cyber-security Policy

- Business continuity plan

- Child Protection and Safeguarding Policy

- Child-on-child Abuse Policy

- Anti-Bullying Policy

- Behaviour and Relationships Policy

- Disciplinary Policy and Procedure

- Data Protection Policy

- Privacy Policy

- Prevent Duty Risk Assessment

- Remote Education Policy

Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

- Ensuring the DSL's remit covers online safety.

- Reviewing this policy on a bi-annual basis.

- Ensuring their own knowledge of online safety issues is up-to-date.

North Star Academy Trust E-Safety Policy

- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

- Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.

- Ensuring online safety practices are audited and evaluated.

- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

- Working with the DSL and ICT technicians to conduct yearly light-touch reviews of this policy.

- Working with the DSL and governing board to update this policy on a bi annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

North Star Academy Trust E-Safety Policy

- Ensuring safeguarding is considered in the school's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.

- Understanding the filtering and monitoring processes in place at the school.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

- Reporting to the governing board about online safety on a bi termly basis.

- Working with the headteacher and ICT technicians to conduct yearly light-touch reviews of this policy.

- Working with the headteacher and governing board to update this policy on a bi annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.

- Implementing appropriate security measures as directed by the headteacher.

- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

- Working with the DSL and headteacher to conduct yearly light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.

- Modelling good online behaviours.

- Maintaining a professional level of conduct in their personal use of technology.

- Having an awareness of online safety issues.

North Star Academy Trust E-Safety Policy

- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.

- Reporting concerns in line with the school's reporting procedure.

- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.

- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

- Reporting online safety incidents and concerns in line with the procedures within this policy.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training

- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation

- Online safety is integrated into learning throughout the curriculum

- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

North Star Academy Trust E-Safety Policy

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages

- Threatening or embarrassing pictures and video clips sent via mobile phone cameras

- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible

- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name

- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

- Abuse between young people in intimate relationships online i.e. teenage relationship abuse

- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment – see NSAT child on child Sexual harassment and sexual harm policy

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence

- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks

- Sexualised online bullying, e.g. sexual jokes or taunts

- Unwanted and unsolicited sexual comments and messages

- Consensual or non-consensual sharing of sexualised imagery

- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

North Star Academy Trust E-Safety Policy

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.

- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "**online hoax**" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "**harmful online challenges**" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge

itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.

- Careful to avoid needlessly scaring or distressing pupils.

- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.

- Proportional to the actual or perceived risk.

- Helpful to the pupils who are, or are perceived to be, at risk.

- Appropriate for the relevant pupils' age and developmental stage.

- Supportive.

- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE

- Relationships and health education

- PSHE

- Citizenship

- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online

- How to recognise techniques used for persuasion

- Acceptable and unacceptable online behaviour

- How to identify online risks

- How and when to seek support

- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in our PSHE scheme of work.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers

- Laptops

- Tablets

- Intranet

- Email

- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's technology Acceptable Use Agreement for Pupils, see Appendix A.

Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Agreement, see Appendix B

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.

North Star Academy Trust E-Safety Policy

- Sharing indecent images, both consensually and non-consensually.

- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.

- Exposure to radicalising content.

- Sharing of indecent imagery of pupils, e.g. sexting.

- Cyberbullying.

- Exposure to age-inappropriate content, e.g. pornography.

- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

North Star Academy Trust E-Safety Policy

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings

- Newsletters

- Online resources

Internet access

Staff and students can only access the internet via the school internet provider via school equipment. Anyone using this system is protected by Netsweeper and has agreed to our acceptable use agreement within our Code of Conduct.
Guests are permitted to use our internet but must agree to our 'acceptable use' before using the Trusts internet.

Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. NSAT currently works with **Soltech** to provide filtering and monitoring through Netsweeper.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

North Star Academy Trust E-Safety Policy

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Full details of the school's network security measures can be found in our agreements with our IT provider.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Privacy Policy and Staff and Volunteer Privacy Policy.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity

North Star Academy Trust E-Safety Policy

within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT technicians share e updates to explain what a phishing email and other malicious emails might look like – this information will include information on the following:

- How to determine whether an email address is legitimate

- The types of address a phishing email could use

- The importance of asking "does the email urge you to act immediately?"

- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the NSAT information security policy.

Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Social networking

The use of social media by staff and pupils will be managed in line with NSAT Social Media Policy and Code of Conduct.

The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

North Star Academy Trust E-Safety Policy

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the 'Staff' and 'Student Acceptable Use' agreement Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct yearly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on a biannual basis and following any online safety incidents.

The next scheduled review date for this policy is Sept 2026.

Any changes made to this policy are communicated to all members of the school community.

PUPIL ACCEPTABLE ICT USE POLICY-Secondary

New technologies have become integral to the lives of young people in today's society, 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and, in return, expects the pupils to agree to be responsible users.

ACCEPTABLE ICT USE POLICY AGREEMENT

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems and devices
- I will keep my username and password safe and secure – I will not share it or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line
- I will not arrange to meet people off-line that I have communicated with on-line without the knowledge and permission of a responsible adult (parent/carer)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line (to a teacher in school or to my parent/carer at home)

I understand that everyone has equal rights to use technology as a resource and:

- I will not use the school systems or devices for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

North Star Academy Trust E-Safety Policy

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I understand that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software
- I will not install or attempt to install or store programmes of any type on any school device or try to alter computer settings.
- I will only use social media sites with permission and at the times that are agreed

When using the internet for research or recreation

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to ICT systems and the internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

I have read and listened to all the information about safe use of ICT at school.

I agree to:

North Star Academy Trust E-Safety Policy

- ☐ Use the school equipment in school
- ☐ Follow safe procedures in school and out of school
- ☐ Use my own ICT equipment outside of school in a way that is expected of me as a member of this school

[ ] Name of pupil:

[ ] Signed:

[ ] Parent / Carer Signature:

[ ] Date:

Appendix A 1

PUPIL ACCEPTABLE ICT USE POLICY- Primary

Stay Safe - computers, phones, consoles!

Computers, phones, consoles give you lots of opportunities to talk to your friends, be creative and to learn new things. You are entitled to be safe all the time. Our school will make sure you have good access to ICT so that you can learn but we want you to agree to be a responsible user of ICT. Our school system is safe and will protect you from anything that may put you at risk.

For your safety we will monitor how you use computers and ICT but we need you to:

- Keep your user name and password safe and secure, this means **not** sharing them and **not** trying to use anyone else's username and password
- Be aware of "stranger danger" when using the Internet
- Keep all personal information, about yourself and other people, private
- Avoid arranging to meet people that I have chatted to on-line without the knowledge and permission of a responsible adult, my parent / carer
- Report any messages or images that make me feel uncomfortable when I see them on-line, to an adult in school or to my parent / carer at home

Everyone has equal rights to use our ICT equipment as a resource, so:

- I will only use ICT when I am given permission to do so

North Star Academy Trust E-Safety Policy

- I will use downloads or uploads for my work and will make sure they are not too big and stop others from doing their work
- I will only use the school system for games if an adult gives me permission to do so

I expect other pupils to act towards me in the way I will act towards them, this means:

I will be polite, I will avoid using

I will not take or send

I will respect others'
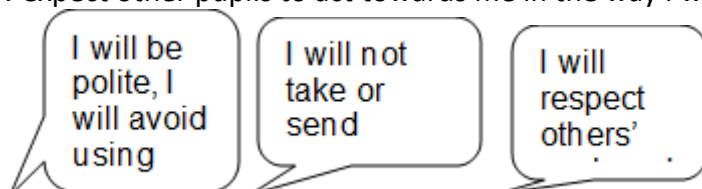
I know my school has a responsibility to keep me safe, to help the school I will:

- Only download information that is legal and will not cause any upset or harm
- Only use the programmes I am allowed to use
- Tell an adult if the equipment or programmes are not working
- Only use specific sites with agreement and when an adult says I am allowed to use those sites

I understand the importance of not copying other people's work and saying it is mine. If I need to I will

- Ask permission to use someone else's work
- Check that information is accurate and is not misleading

I understand that I have to be responsible for my actions both in school and out of school. My school can take action if I am involved in something that reflects badly on my school e.g. cyber-bullying, or sending out pictures and personal information about other people. If I don't use ICT safely I could lose my right to use our equipment, my parents/ cares will be informed and if necessary, the police may become involved.

North Star Academy Trust E-Safety Policy
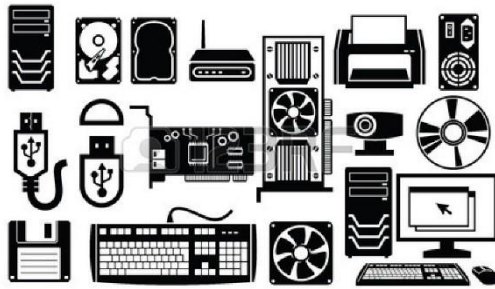
I have read and listened to all the information about safe use of ICT at school.

I agree to:

- ☐ Use the school equipment in school
- ☐ Follow safe procedures in school and out of school
- ☐ Use my own ICT equipment outside of school in a way that is expected of me as a member of this school

Name of pupil:

Signed:

Parent / Carer Signature:

Date:

Appendix B

Staff and Volunteer Acceptable Use Policy Agreement

Safeguarding statement*:*

Nothing contained within this policy overrides the current and on-going commitment of the trust to adhere to the Safeguarding of children, vulnerable adults or members of staff. This policy along with all others should be read in conjunction with the schools **'Safeguarding'** policy.

Safeguarding of the children, vulnerable adults and members of staff is at the forefront of everything we do.

Trust Policy

New technologies have become integral to the lives of children and young people in today's society, 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This policy extends to communication outside of the schools.

This Acceptable Use Policy is intended to ensure:

That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

That the schools ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

That staff are protected from potential risk in their use of ICT in their everyday work.

The schools will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use schools ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

North Star Academy Trust E-Safety Policy

☐ I understand that the schools may monitor my use of the ICT systems, email and other digital communications.

☐ I understand that the rules set out in this agreement also apply to use of schools ICT systems (e.g. laptops, email, VLE etc) out of school.

☐ I understand that the schools ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the schools.

☐ I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

☐ I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

I will ensure that I only use the schools camera equipment to photograph or record the children and that such cameras will remain in the schools except for use as part of a field trip or excursion. I further understand that the images from such cameras will be stored on school systems unless express permission has been obtained from the Head Teacher or senior member of staff.

I will be professional in my communications and actions:

☐ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

☐ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

☐ I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

☐ I will not use chat and social networking sites on schools equipment.

☐ I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. Further to this I will never give out my personal address, mobile phone number etc or that of other members of staff/school community without their express permission.

☐ I will not engage in any on-line activity either at home or in school that may compromise my professional responsibilities including but not limited to using social networking sites to discuss grievances relating to work or children, members of staff, comments, confidential matters or any activity that may bring the school into disrepute.

I will ensure that I abide by the rules set out by the owners of social networking sites or when using communication media and will also ensure that I do not have either former or current pupils listed as friends, associates or otherwise engage in communicating with pupils or ex-pupils in a manner that may allow or by inaction allow myself or the school to be brought into disrepute, be placed in a vulnerable position or be open to litigation.

I will use an encrypted memory stick to store information relating to the children. The use of non-encrypted memory sticks or devices for the transportation or holding of personal pupil data is strictly forbidden.

I will ensure that I only use schools email addresses to communicate with school staff or outside organisations when the main reference is relating to the children of the schools either present or past. I will not send unencrypted information via email at any time.

I will ensure that I only use school fixed line or school mobile telephones to communicate with parents or pupils and will not use personal fixed line telephones or mobile devices.

The schools and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schools:

☐ When I use my personal hand held/external devices (PDAs laptops mobile phones USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using schools equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

☐ I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

☐ I will ensure that my data is regularly backed up, in accordance with relevant school policies.

☐ I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

☐ I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

☐ I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or given specific permission.

☐ I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others. Where personal data is transferred outside the secure school network, it must be secured in such a way that members of the general public cannot access it.

☐ I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

☐ I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

North Star Academy Trust E-Safety Policy

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Trust Board and/or the Local Authority, dismissal and in the event of illegal activities the involvement of the police.

Staff and Volunteer Acceptable Use Policy

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name

Signed

Date

Appendix C

NSAT Visitor Acceptable Use Agreement

Safeguarding statement*:*

This policy along with all others should be read in conjunction with the schools **'Safeguarding'** policy.
Safeguarding of the children, vulnerable adults and members of staff is at the forefront of everything we do.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That the schools ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The schools will try to ensure that volunteers will have good access to ICT to enhance their work, in return we expect volunteers to agree to be responsible users.

Acceptable Use Agreement

The schools and has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schools:

- When I use my personal hand held/external devices (PDAs laptops mobile phones USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using schools equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or given specific permission.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others. Where personal data is transferred outside the secure school network, it must be secured in such a way that members of the general public cannot access it.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

North Star Academy Trust E-Safety Policy

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Visitor Acceptable Use Policy

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Visitor name

Signed

Date

Please see reception once this agreement is signed for log on details.

North Star Academy Trust E-Safety Policy

Appendix D

The use of AI in NSAT Schools

1 PURPOSE

1.1 The purpose of this appendix document is to establish guidelines for the ethical, secure and responsible use of Artificial Intelligence (AI) technologies in our school community. It is designed to provide a framework for the appropriate use of AI technologies while ensuring that students' privacy, security and ethical consideration are taken into account.

2 SCOPE

2.1 This appendix applies to all members of our school community, including students, teachers, administrative staff and other stakeholders who may use AI technologies in the school environment. It particularly covers, although is not limited to, generative AI technologies, such as large language models (LLMs).

2.2 The following stakeholders are involved in the implementation of this policy: school leadership, teachers, administrative staff, students, and parents/guardians.

3 APPENDIX STATEMENT

3.1 The Trust is committed to using AI technologies in an ethical, transparent and responsible manner. We acknowledge that AI technologies have the potential to significantly enhance student learning and engagement, but we also recognise the importance of protecting student privacy and ensuring that the use of these technologies is consistent with ethical considerations.

3.2 The use of AI technologies across the Trust aligns with our mission to provide a high-quality and relevant education that prepares students for their next steps and adulthood. AI technologies have the potential to support personalised learning and help teachers identify areas where students need extra support, for example provide personalised direction towards resources in particular. It also has the potential to support in analysing student data to tailor instruction, content, and pacing to individual needs. These tools have the potential to assist teachers in identifying specific learning gaps, and can provide immediate feedback, and automating administrative tasks, allowing educators to focus on targeted support. Generic examples of this technology are Dreambox and Duolingo and elements of Microsoft Co-pilot. The automation of planning and administrative tasks is a focus of Oak Academy, a government sponsored AI technology called Aila.
They can also support research and writing activities and provide opportunities for students to develop skills related to critical thinking, problem solving and digital literacy. It has the potential to support with summarising complex documents, brainstorming ideas, and providing real-time grammar or structure feedback. It can support critical thinking through engagement with large language models and can support digital literacy by critical evaluation of AI-generated content.

4 RESPONSIBILITIES

4.1 The following individuals and groups are responsible for the implementation and maintenance of the guidance:

-School leadership: responsible for providing resources, guidance and support for the implementation of the guidance.

-Teachers: responsible for implementing the guidance in their classrooms, including providing instruction on the ethical and responsible use of AI technologies.

-Administrative staff: responsible for ensuring that AI technologies are used in compliance with this guidance, including data privacy and security policies.

-Students: responsible for using AI technologies in an ethical and responsible manner, as outlined in this guidance.

North Star Academy Trust E-Safety Policy

-Parents/Guardians: responsible for supporting their children's appropriate and ethical use of AI technologies in compliance with this guidance.

-Governors and trustees: responsible for ensuring that AI technologies are used in compliance with this guidance, including data privacy and security policies.

5 ETHICAL CONSIDERATIONS, TRANSPARENCY AND ACCOUNTABILITY

5.1 NSAT recognises the potential benefits of integrating artificial intelligence (AI) technologies into the educational environment. This guidance outlines the principles and guidelines for the responsible use of AI within the school community, in accordance with the standards set forth by the Joint Council for Qualifications (JCQ) and the Department for Education (DfE). (see section 9 below).

5.2 The Trust and its schools will communicate how AI technologies are being used, providing information about the purpose, functionality, and potential impact on students and staff. As outlined above there are clear lines of accountability for the use of AI technologies within the school to ensure proper oversight and decision-making.

5.3 There will always be human oversight and control over any AI systems, particularly in decision-making processes that may impact students' education. We will ensure that staff and students are adequately trained to understand and interpret the outputs of AI technologies including its limitations and potential bias. We will regularly assess any AI systems for bias that may result in unfair treatment of certain individuals or groups, especially with regard to aspects like gender, ethnicity or socio-economic status.

6 DATA PRIVACY AND SECURITY

6.1 The Trust will adhere to data protection laws as outlined in our data protection policy to ensure the privacy and security of student and staff data. Any data collected through AI technologies will only be used for legitimate educational purposes.

6.2 Prior to the use of AI technologies involving data collection, informed consent will be obtained from students, parents, or legal guardians. The purpose, scope and implications of data usage will be clearly communicated.

7 ACCESS AND EQUITY

7.1 AI technologies implemented across the Trust will be designed and used in a manner that promotes equity and inclusion.

7.2 Efforts will be made to ensure that AI technologies are accessible to all students, regardless of abilities or disabilities. The school will work towards removing barriers to access and providing necessary accommodations.

7.3 The deployment of AI technologies will be done in a manner that ensures equitable access to educational resources and opportunities for all students.

8 ACCEPTABLE USE

8.1 The Trust recognises the fundamental importance of student wellbeing and the safe use of the internet. Students should only use AI in a safe and responsible manner. Staff must educate students on the safe use of AI and the internet. The school's safeguarding and e-safety policies must be followed to ensure the safety and wellbeing of students.

8.2 Clear guidelines will be communicated for the acceptable use of AI technologies within the Trust. Users will be educated on responsible and ethical use.

8.3 The Trust prohibits the use of AI technologies for any activities that violate laws, regulations, or ethical standards. This includes but is not limited to cheating, plagiarism, and any form of academic dishonesty.

North Star Academy Trust E-Safety Policy

8.4 The trust is cognisant of Keeping Children Safe in Education (KCSIE) 2026 guidance which explicitly incorporates artificial intelligence (AI) as a key safeguarding area. Our staff will be supported to manage risks such as deepfakes, AI-generated misinformation, and potential grooming. The school filtering system is robust enough to manage these potential threats however staff will need to be vigilant.

9 ACADEMIC INTEGRITY

9.1 AI can be used as an aid for academic purposes, such as research, homework, and assignments, where permitted by the teacher. However, it is essential to note that students should not solely rely on AI to complete their work. The use of AI must be in line with academic integrity guidelines as outlined in this policy and underpinned by the JCQ guidance.

-AI must not be used in exams, as this constitutes exam malpractice.
-Students must not use AI to answer exam questions or seek assistance during the exam.
-Staff should ensure that students are aware of this policy and the consequences of violating it.

Please reference the JCQ guidance here:

https://www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/

9.2 The Trust is committed to upholding academic integrity. Students are prohibited from using AI technologies to engage in cheating or plagiarism. Clear consequences will be outlined for academic misconduct related to AI use.

9.3 Examples of AI misuse include, but are not limited to, the following:

-Copying or paraphrasing sections of AI-generated content so that the work is no longer the student's own.

-Copying or paraphrasing whole responses of AI-generated content.
-Using AI to complete parts of the assessment so that the work does not reflect the student'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 misleading acknowledgment of AI tools.
-Submitting work with intentionally incomplete or misleading references of bibliographies.

9.4 Suspected breaches of academic integrity related to the use of AI technologies will be treated in line with our behaviour policy and / or examinations / non-examinations policies as appropriate. Any breaches of the policy will result in disciplinary action.

10 ASSESSMENT PROCESSES

10.1 As has always been the case, students must submit work for assessments which is their own. This means both ensuring that the final product is in their own words and is not copied or paraphrased from another source such as an AI tool, and that the content reflects their own independent work.

10.2 AI tools must only be used when the conditions of the assessment permit the use of the internet and where the student is able to demonstrate that the final submission is the product of their own independent work and independent thinking.

10.3 The school aligns with the JCQ guidelines AI Use in Assessments: Protecting the Integrity of Qualifications. The AI policy should be read in conjunction with this document.

11 CITATION AND REFERENCING

11.1 It is essential that students reference the sources they have used when producing assessed work. Where students use AI for assessed work, they must acknowledge its use and show clearly how they have used it. Students

North Star Academy Trust E-Safety Policy

and staff should be clear that AI-generated content is not subject to the same academic scrutiny as other published sources and therefore they must exercise caution.

11.2 Where AI tools have been used as a source of information, a student's acknowledgement must show the name of the AI source and should show the date the content was generated. Further guidance regarding citation and referencing can be found in the JCQ guidelines highlighted above.

12 ACCURACY AND CREDIBILITY

12.1 Teachers and students should be aware that AI tools are still being developed and there are often limitations to their use, such as producing inaccurate, misleading or inappropriate content.

12.2 AI-generated information needs to be scrutinised for accuracy and credibility before it is used for educational purposes. Teachers will guide students in critically evaluating AI-generated information and understanding its limitations.

12.3 AI-generated content should be fact-checked using these specifics: the author of the source material, the website's or author's credentials, what the original source says and in what context, the reason why the information was shared, if there are biases present, how recent the information or study was published, and who else is citing the source.

13 PROFESSIONAL DEVELOPMENT

13.1 Staff will receive training on the use of AI technologies in education. Professional development opportunities will emphasise the ethical use of AI technologies, ensuring that educators are proficient in guiding students towards responsible AI usage.

13.2 NSAT is committed to looking for opportunities to use AI which will bring about benefits for teachers and students. For example, teachers may want to make use of AI to create and support lesson resources. We will continue to explore ways to use AI to reduce workload however this will not be done at the expense of personalisation and never take the place of the teacher's professional judgement on how to personalise resources.

14 COMMUNITY ENGAGEMENT

14.1 The school will engage with members of the school community to inform them about the use of AI technologies for educational purposes. As part of our regular surveys, feedback from students, parents and staff will be considered in the ongoing evaluation and development of AI use in school.

15 REVIEWING AND UPDATING THE POLICY

15.1 This AI appendix is developed in compliance with the guidelines provided by the Joint Council for Qualifications (JCQ), the Department for Education (DfE) and NSAT.

15.2 The Trust is committed to regularly reviewing and updating this AI appendix and align with emerging best practices, technological advancements, and changes in regulations.

15.3 The Trust will regularly assess the ethical implications of AI technologies and be prepared to make adjustments or discontinue the use of certain technologies if ethical concerns arise.

16 CURRENT RECOMMENDED AI TOOLS
16.3 There are a range of AI tools available for the teachers to use however the one that the Trust recommends is Oak Academy and the AI tool within it called Aila. If other AI tools are being used teachers need to use their professional judgement and check that anything AI generates is accurate and appropriate. It is the responsibility if the teachers to ensure that the tools they use follow the legal requirements around data protection, child safety and intellectual

property. If staff are unsure about if they should be using an AI tool then they should check with the leadership in their school.

17 ADDITIONAL READING

https://educationhub.blog.gov.uk/2025/06/artificial-intelligence-in-schools-everything-you-need-to-know/
https://assets.publishing.service.gov.uk/media/6842e04ee5a089417c8060c5/Leadership_Toolkit_-_Transcript.pdf
https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education
https://www.gov.uk/government/publications/generative-ai-product-safety-standards/generative-ai-product-safety-standards#filtering