



Online Safety Policy

Date Published	March 2024
Version	3
Approved Date	March 2026
Review Cycle	Annual
Review Date	March 2027

An academy within:



“Learning together, to be the best we can be”

1. Purpose

- 1.1. Set out the key principles expected of all members of the school community at Kenwood Academy with respect to the use of ICT-based technologies.
- 1.2. Safeguard and protect the children and staff of Kenwood Academy.
- 1.3. Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- 1.4. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use, as outlined and agreed in the Nexus Acceptable Usage Agreement.
- 1.5. Have clear structures to deal with online abuse such as cyberbullying.
- 1.6. Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- 1.7. Have identified a clear route of complaint against any misplaced or malicious allegations made against any member of the school community.

2. Main Areas of Risk

2.1. Content (not exhaustive):

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, sexting.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content

2.2. Contact:

- Grooming.
- Cyber-bullying in all forms.
- Identity theft (including 'frape', hacking Facebook profiles) and sharing passwords.

2.3. Conduct:

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online, internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

3. Scope

- 3.1. This policy applies to all members of Kenwood Academy community (including staff, students, volunteers, parents/carers and visitors) who have access to and are users of the academy ICT systems, both in and out of Kenwood Academy.
- 3.2. The Education and Inspections Act empowers Co-Headteachers and members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school/academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.
- 3.3. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

4. Key Roles and Responsibilities

Trustees

- 4.1 The Policy Review Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Trust board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- 4.2 All Trustees will:
 - Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or academy approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- Trustees will review the DfE's filtering and monitoring standards, and discuss with IT staff and Trust leadership what needs to be done to support the school in meeting the standards.

The Academy Council

- 4.3. Governors will be aware of how staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

Executive Headteacher

- 4.4. The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

- 4.5. Details of the school's DSL and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Executive Headteacher to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT Engineer to make sure the appropriate systems and processes are in place.
- Working with the Executive Headteacher, ICT Engineer and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Executive Headteacher and/or Academy Council.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

The Online Safety Coordinator / E-Safety Officer

4.6. The Online Safety Coordinator will:

- Take day to day responsibility for online safety issues and works closely with the DSL in establishing and reviewing the school's online safety policy and documents.
- Promote an awareness and commitment to E-safeguarding throughout the school community.
- Ensure that online safety education is embedded across the curriculum.
- Liaise with school ICT technical staff.
- Communicate regularly with ALT, DSL to discuss current issues, review incident logs and filtering / change control logs.
- Is regularly updated in online safety issues and legislation, and is aware of the potential for serious child protection issues to arise from:
 - sharing of personal data
 - access to illegal / inappropriate materials
 - inappropriate on-line contact with adults / strangers
 - potential or actual incidents of grooming
 - cyber-bullying and use of social media

Computing Lead

4.6. Overseeing the delivery of the online safety element of the Computing curriculum.

4.6.1. Liaising with the On-line Safety Co-ordinator regularly.

The ICT Engineer

4.7. Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess

effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

- Ensuring that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems.
- Ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Keeping up to date with this policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

This list is not intended to be exhaustive.

Data Processor

4.8. Ensure that all data held on students on the school office machines have appropriate access controls in place, and that processes are Data Protection Act (2018) compliant.

4.8.1. Ensure all staff and students have signed an acceptable user agreement form and understands that they must report any concerns.

Nexus Multi Academy Trust

4.9. Ensure all Trust services are managed on behalf of the school.

4.9.1. Ensure that the school's policy on web filtering is applied and updated on a regular basis.

Teachers

4.10. Embed online safety issues in all aspects of the curriculum and other school activities.

4.10.1. Supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

4.10.2. Ensure that students are fully aware of research skills and are fully

aware of legal issues relating to electronic content such as copyright laws.

All Staff and Volunteers

4.11. All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and implementing it consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the Online Safety Co-ordinator and DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Families

4.12. Our families are expected to:

- Notify a member of staff of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Families can seek further guidance on keeping children safe online from the following organisations and websites:

[What are the issues? - UK Safer Internet Centre](#)
[Help & advice | Childnet](#)
[Parents and Carers resource sheet | Childnet](#)

Visitors and members of the community

4.13. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant,

and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Generative Artificial Intelligence

- 5.1. Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
- 5.2. Kenwood Academy recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- 5.3. Kenwood Academy will treat any use of AI to bully pupils in line with our behaviour policy.
- 5.4. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.
- 5.5. In line with the Trust Information Governance policy, schools should note that if personal and/or sensitive data is entered into an unauthorised generative AI tool, Nexus will treat this as a data breach and will follow the personal data breach procedure.

6. Educating and Supporting Children about Online Safety

6.1 Our Pupils will be taught about online safety as part of the curriculum:
All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact
Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That

social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online

- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion,

how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion

- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

7. Online Safety Curriculum

7.1. Kenwood Academy has a clear, progressive online safety education programme as part of the curriculum. This covers a range of skills and behaviours appropriate to age and experience. Students will be taught to:

- STOP and THINK before they CLICK.
- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Understand acceptable behaviour when using an online environment / email.
- 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 any files – such as music files - without permission;
- Recognise inappropriate content, contact and conduct, and know how to report concerns.
- How to report a range of concerns.

8. Educating our families about online safety

8.1. The school will raise family's awareness of internet safety in letters or other communications home, and in information via our website. If families have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Executive Headteacher.

9. Acceptable use of the internet in school

- 9.1. All students, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Our systems monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. The Executive Headteacher, DSL, Online Safety Co-ordinator and IT Engineer are alerted to any breaches of this.

10. Students using mobile phones in school

- a. All students are expected to follow school guidelines on mobile phones. Guidance can be found on the school website.

11. Monitoring

- 11.1 The DSL logs behaviour and safeguarding issues related to online safety.
- 11.2 DSL should take lead responsibility for auditing the effectiveness of the filtering and monitoring systems.
- 11.3 Staff and volunteers should oversee and monitor all online access/usage and challenge/report any misuse.
- 11.4 This policy will be reviewed every year by the head teacher. At every review, the policy will be shared with the Policy Review Board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

12. Links with other policies

- 12.1 This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy