Online Safety Policy

Date Published	**March 2024**
Version	**1**
Approved Date	**March 2024**
Review Cycle	**Annual**
Review Date	**March 2025**

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

The Academy Council

4.1. 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.

Co-Headteacher

4.2. The Co-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)

4.3. 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 Co-Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Co-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 Co-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 Co-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

4.4. 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 SLT, 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 E-Safety Officer 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) complaint.

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 E-Safety Officer 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. Online Safety Curriculum

5.1. 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.

6. Educating our families about online safety

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 Co-Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Co-Headteacher.

7. Acceptable use of the internet in school

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 Co-Headteacher, DSL, E-Safety Officer and IT Engineer are alerted to any breaches of this.

8. Students using mobile phones in school

All students are expected to hand in their mobile phones to staff at the start of the school day; or to keep them safely stored out of sight and to not use them throughout the school day.

9. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every year.

10. Links with other policies

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