Pennine View

Online Safety Policy

Date Published	**April 2017**
Version	**4**
Approved Date	**October 2023**
Review Cycle	**Annual**
Review Date	**October 2024**

An academy within:

nexus
Multi Academy Trust

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

1. Introduction and Overview

1.1. 'It Could Happen Here' - All staff including leaders hold firmly in their mind 'it could happen here' and therefore place the best interests of the child at the forefront of all that we do. The school processes and systems ensure that we have positive respectful culture. Leaders and staff are vigilant and alert therefore reporting is timely. School provides education to both pupils and staff so that we can be as up to date as possible.

1.2. Abuse is the form of maltreatment of a child. Somebody my abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in an institutional or community setting by those known to them or, more rarely by others. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children. Online safety is a feature in all areas of abuse: sexual abuse, neglect, physical abuse, emotional abuse and County lines where children are increasingly being targeted and recruited online through social media.

1.3. The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Pennine View School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Pennine View School.
- 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.
- 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 AUP.
- Have clear structures to deal with online abuse such as cyberbullying.
- 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.
- Have identified a clear route of complaint against any misplaced or malicious allegations made against any member of the school community.

1.4. The main areas of risk for our school community can be summarised as follows:

1.5. Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games/films (exposure to violence associated with often racist language), substance abuse, youth produced sexual imagery.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.

- Content validation: how to check authenticity and accuracy of online content

1.6. Contact

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

1.7. 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).
- Youth produced sexual imagery (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) or sexting.
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).
- (Ref KCSIE 2018/NSPCC)

2. Scope

2.1. This policy applies to all members of Pennine View School 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 Pennine View School.

2.2. The Education and Inspections Act empowers Headteachers 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.

2.3. 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 take place out of school.

3. Key Responsibilities

3.1. Headteacher

- Ensures the school implements appropriate ICT systems and services, including school-safe filtering and monitoring, and protected email systems.
- Ensure all technology usage is implemented according to child-safety first principles.
- To be responsible for ensuring that staff receive suitable training to carry out their safeguarding and online safety roles.
- Oversee the activities of the DSL and ensure that their responsibilities are being followed and fully supported.
- Ensure the policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance.
- Liaise with DSL / DDSL on all online safety issues that might arise and keep abreast with updates on school issues and broader policy and practice information.
- To take overall responsibility for data and data security as per the Trust Information Governance Policy.
- To have overall responsibility as data controller.

3.2. Designated Safeguarding Lead (DSL)

- Can delegate online safety duties although the overall responsibility remain with them.
- Takes the lead responsibility for safeguarding and child protection, including online safety.
- Ensure there is regular review and communication between roles.
- Ensure there is correct liaison with the appropriate authorities and work with other agencies in line with local procedures and laws.
- Has overall responsibility for any arising online safety issues and must take a proactive approach to the potential for serious safeguarding issues.
- Have a duty alongside SLT members to ensure that protection of children is paramount and is always put first.
- Ensure they stay up to date with current trends and issues in relation to online safety.
- Must be aware of any updates or changes regarding online safety issues and legislation.
- They have a duty to ensure that online safety education is embedded across the curriculum and into wider school life.
- Promote an awareness and commitment to online safety throughout the school community including parents.

- Communicate regularly with SLT, Governors in respect of current issues, review incident logs and discuss how effectively filtering and monitoring is working in the school.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident and are logged using CPOMS.

3.3. Online Safety Lead (OSL)

- Takes day to day responsibility for online safety and has a leading role in establishing and reviewing the school relevant policies / documents.
- Promotes an awareness and commitment to online safety throughout the school community.
- Ensures that online safety education is embedded across the curriculum.
- Liaises with school ICT technical staff.
- To communicate regularly with SLT, DSL and the designated Online Safety Governor to discuss current issues and filtering.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Facilitates training and advice for all staff.
- Liaises with the Nexus Trust/LA and relevant agencies.
- Is regularly updated in online safety issues and legislation, and be 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

3.4. Governors/safeguarding link governor

- A member of the Governing Body has taken on the role of safeguarding link governor to ensure that the school follows all current Online safety advice to keep the children and staff safe.

3.5. ICT Lead

- To oversee the delivery of the Online safety element of the Computing curriculum.
- To liaise with the Online safety lead regularly.

3.6. Network Manager/Engineer

- To report any online safety related issues that arises, to the online safety coordinator/DSL.
- To ensure that users may only access the school’s networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.

- To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date.
- To ensure the security of the school ICT system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.
- That the engineer keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network/Virtual Learning Environment (LEARNING PLATFORM)/ remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to the Online safety Co-ordinator/Headteacher for investigation, action and/or sanction.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up-to-date documentation of the school's and Nexus Trust's E-Security and technical procedures.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.

3.7. Data Manager

- To ensure that all data held on pupils on the school office machines have appropriate access controls in place, and that processes are GDPR compliant.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.

3.8. Teachers

- To embed Online safety issues in all aspects of the curriculum and other school activities.
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant).
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

3.9. All Staff

- To read, understand and help promote the school's safeguarding, child protection and online safety policies and guidance.
- Recognise that children are capable of abusing their peers.
- Will respond to all reports and concerns of peer-on-peer sexual violence and sexual harassment, including those that have happened outside of school and /or online.

- To read, understand, sign and adhere to the Nexus Trust Acceptable Use Agreement.
- To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- To report any suspected misuse or problem to the Online Safety Lead / DSL.
- To maintain an awareness of current online safety issues and guidance e.g. through assemblies, bulletins, newsletters, CPD sessions.
- To model safe, responsible and professional behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

3.10. Pupils

- Read, understand, sign and adhere to the Student/Pupil Acceptable Use Guidelines.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking/use of images and on cyber-bullying.
- To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To help the school in the creation/ review of online safety policies. To help the school in the creation/ review of Online safety policies.

3.11. Parents/Carers

- To support the school in promoting Online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images.

- To read, understand and promote the school Pupil ICT guidelines (as above) with their children.
- To access the school website learning platform, on-line student, pupil records in accordance with the relevant school Acceptable Use Guidelines.
- To consult with the school if they have any concerns about their children's use of technology.

4. Communication

4.1. How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Acceptable Use Agreements discussed with pupils at the start of each year.
- Acceptable Use Agreements to be kept in personnel files

5. Complaints

5.1. The school will take all reasonable precautions to ensure effective online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Nexus Trust can accept liability for material accessed, or any consequences of Internet access.

5.2. Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview by Head of key stage/ Head/Deputy head teacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period.
- Referral to LA / Police.

5.3. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school, Nexus Trust and LA child protection procedures.

6. Education and Curriculum

6.1. Pupil online safety curriculum

6.1.1. This school as a clear, progressive online safety education programme as part of the Computing curriculum / RSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To 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;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand the signs and dangers of 'grooming'.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming/gambling.

6.2. Sexual Imagery

6.2.1. The law states that making, possessing and distributing any imagery of someone under 18 which is 'indecent' in an offence. This includes imagery of yourself if you are under 18. The Sexual Offences Art 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. Schools may respond to incidents without involving the police. The DSL will consider a range of information and through discussion with Headteacher before making a decision whether the incident is reportable to the Police. Where the police are notified of incidents, they are obliged to record the incident on their crime systems.

6.2.2. School defines sexual abuse imagery as:

- A person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18.
- A person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18.
- A person under the age of 18 in possession of nudes and semi nudes created by another person under the age of 18.

6.3. Online Safety Incident

- Online safety reports will be managed by two members of staff present, one person must be either the DSL or DDSL.
- Staff must not view or forward illegal images of a child. We respect the dignity of the child.
- In some cases, the school may take the decision to confiscate any devises to preserve any evidence and hand them to the police for inspection.

6.4. Staff and Governor Training

6.4.1. This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on Online safety issues and the school's Online safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and

guidance on the Online Safety policy and the school's Acceptable Use Guidelines.