E-Safety Policy

Date Published	**November 2019**
Version	**2**
Approved Date	
Review Cycle	**Annually**
Review Date	**November 2020**

An academy within:

nexus Multi Academy Trust

1. Introduction and Overview

Rationale

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.

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

Content (Including but not exhausted)

- 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

Contact

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

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).

(Ref KCSIE 2018/NSPCC)

Scope

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.

The Education and Inspections Act empowers Head teachers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-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.

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 e-safety behaviour that take place out of school.

2. Key Responsibilities

Headteacher/DSL

- To take overall responsibility for E-Safety provision
- To take overall responsibility for data and data security (SIRO)
- To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements.
- To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.
- To be aware of procedures to be followed in the event of a serious e-Safety incident.
- To ensure that there is a system in place to monitor and support staff that carry out internal e-safety procedures.
- To have overall responsibility as data controller.

E-Safety Lead

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

Governors/E-Safety linked Governor

- A member of the Governing Body has taken on the role of E-Safety Governor.
- To ensure that the school follows all current E-Safety advice to keep the children and staff safe.
- To review the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports.
- The role of the E-Safety link Governor will include:
    - Annual review with the E-Safety Lead, including reviewing E-Safety incident logs, filtering /change control logs

ICT Lead

- To oversee the delivery of the E-Safety element of the Computing curriculum.
- To liaise with the E-Safety lead regularly.

Network Manager/Engineer

- To report any e-Safety related issues that arises, to the e-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 e-safety policy and technical information in order to effectively carry out their e-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 E-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.

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.

Nexus Trust

- To ensure all Nexus Trust services are managed on behalf of the school.
- The school's policy on web filtering is applied and updated on a regular basis.

Teachers

- To embed E-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.

All Staff

- To read, understand and help promote the school's e-Safety policies and guidance.
- To read, understand, sign and adhere to the Nexus Trust Acceptable Use Agreement.
- To be aware of e-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 e-Safety coordinator/DSL.
- To maintain an awareness of current e-Safety issues and guidance e.g. through CPD.
- 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.

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 e-safety practice when using digital technologies out of school and realise that the school's E-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 e-safety policies. To help the school in the creation/ review of E-Safety policies.

Parents/Carers

- To support the school in promoting E-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.

Communication

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

Handling Complaints:

- The school will take all reasonable precautions to ensure e-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.

- 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.

- 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.

Review and Monitoring

The e-safety policy is referenced from within other school policies: safeguarding, Behaviour Policy, Anti-Bullying policy and Staff Code of Conduct.

- The school has an e-safety lead who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

3. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE 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.

Staff and Governor Training

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 E-Safety issues and the school's E-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 E-Safeguarding policy and the school's Acceptable Use Guidelines.