Online Safety Policy 2023-24

Background

Schools must be highly aware of online safety and make both staff and students aware of the dangers of using electronic communication as well as its undoubted benefits. The DfE non-statutory guidance 'Teaching online safety in schools' June 2019 is a helpful document for assisting teachers in the delivery of online safety education.

The DfE's statutory guidance 'Keeping Children Safe in Education' (September 2023) outlines the responsibilities that schools and colleges have in safeguarding children including reference to online safety.
The document requires schools to ensure that:

- Students are taught about safeguarding, especially against online abuse such as bullying and sexual abuse by exploitation online.
- They have appropriate filtering and monitoring systems in place on the school's ICT systems so that no student can access harmful content.
- They are careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- They develop methods whereby staff are alerted to changes in children's behaviour which could indicate that they may need help or protection from child protection issues via the internet or social media.
- Staff should use their judgement and act proportionately, which may include making a referral to the Channel programme under the school's prevent duty.
- To protect and educate students and staff in their use of technology.
- To have the appropriate mechanisms to intervene and support any incident where appropriate. The briefing paper states that the breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
- Content – being exposed to illegal, inappropriate, or harmful material.
- Contact – being subjected to harmful online interaction with other users.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm.

With regard to the online safeguarding of students, inspection will include:

- Look for evidence that appropriate filters and monitoring systems are in place to protect students from potentially harmful online material.
- Discuss online safety in their discussions with students (covering topics such as online bullying and safe use of the internet and social media).

- Will investigate what the school does to educate students in online safety and how the school deals with issues when they arise.

Personal data held or processed by the School Under the General Data Protection Regulation schools are responsible for higher standards of online safety and security of all personal data that they process. Inspectors will consider schools' compliance with these regulations when conducting school inspections.

Introduction

Today's students are growing up in a world where online and offline life is almost seamless. This offers many opportunities but also creates challenges, risks and threats that need students need to be guided through. At Northleigh House School, we try to equip our students with the knowledge to be able to use technology to their best advantage in a safe, considered, and respectful way.

Our school community recognises the importance of treating online safety as an ever-present serious safeguarding issue, and its teaching is a whole school issue and the responsibility of all staff. It is important to protect and educate both students and staff and have supportive mechanisms, policies, and protocols in place to protect and support the school community.

Inspections review online safety measures in schools and there are numerous Acts of Parliament which relate when considering the safeguarding of both staff and students in schools.

The safeguarding aspects of online safety are evident in all our ICT/safeguarding policies and procedures throughout the school. It is essential that this constantly developing area of technology is kept under review. It is also critical to ensure the safety and security of all personal data that the school holds and processes. Under the General Data Protection Regulation, the school is responsible for exacting standards of safety and security of personal data that may be processed. This policy links all the ICT, safeguarding and other policies and procedures to reflect how the school deals with online issues daily.

This policy is aimed at making the use of electronic communication at Northleigh House School as safe as possible. This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems both in and out of school.

Action plan

The school will deal with any online safety incidents which arise by invoking this policy, other ICT policies and the associated behaviour policies which include dealing with anti-bullying. The school will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place inside or out of school and take appropriate action. Any breaches of safety of personal data held by the school that may arise will be dealt with as soon as they come to light and the appropriate authorities notified.

The following sections outline:

- The roles and responsibilities for online safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles.
- How the infrastructure is managed.
- How online safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.
- Awareness of and dealing with inappropriate use of electronic media.

Roles and Responsibilities – Trustees

- Filtering and monitoring are important parts of the online safety picture at Northleigh House School and the governors ensure that appropriate filters and monitoring systems are in place on the school's ICT resources. Moreover, the trustees have a whole school approach to online safety, which includes policies and procedures on mobile technology use in the school. Some students have access to the internet through smart devices unfiltered by the school. The school's policy on confiscation of inappropriate items will be used if it is found that such devices are being use inappropriately on the premises.
- Trustees will ensure compliance with the Data Protection Act and GDPR.
- Trustees will ensure that students are taught about online safety, for example through personal, social, health and economic education (PSHE) and through relationships and sex education (RSE).
- Trustees are responsible for the approval of the Online Safety Policy, for reviewing the effectiveness of the policy and for dealing with issues when they arise.
- Trustees receive online safety training/awareness.

Roles and Responsibilities – School Director and Senior Leaders

- The School Director and Senior Leaders are responsible for ensuring the online safety of members of the school community and will manage the education of students and training of staff in online safety and awareness of potential child protection issues in students.
- The School Director and Senior Leaders will take appropriate action if it is felt that any student or member of staff of the school may be becoming radicalised or there are any child protection issues.
- The School Director and Senior Leaders, together with the Data Protection Officer, is responsible on a day-to-day basis for ensuring compliance with the Data Protection Act and GDPR for the processing of personal data.
- The School Director, Senior Leaders and Network Manager will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including the School Director.
- The Education and Inspections Act 2006 empowers the School Director and Senior Leaders to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers 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, even though they may take place out of school, but are linked to membership of the school.

Roles and Responsibilities – Senior Designated Safeguarding Lead (SDSL)

- Leads and coordinates the works with key staff which consists of SDSL, Network Manager, Computing Department, Wellbeing Team and the Safeguarding Trustee.
- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's Online Safety Policy and other related policies, including the safe processing of personal data.
- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff to ensure that all teaching is carried out in an age-appropriate way and that staff are trained in how to stay safe online.
- Will access training and professional development as deemed appropriate or necessary in response to education and/or technological developments and by reviewing national and local guidance documents.
- Liaises with the local authority (LA) and reports to the Chair of Trustees any suspicions of students who may be becoming radicalised. The Senior Designated Safeguarding Lead is trained in online safety issues and will be aware of the potential for serious child protection issues to arise from:
    - Sharing of personal data.
    - Access to illegal/inappropriate materials.
    - Inappropriate online contact with adults/strangers.
    - Potential or actual incidents of grooming.
    - Cyber-bullying.
    - Sexting.
    - Suspicions of radicalisation.

  This is not an exhaustive list.

Roles and Responsibilities – Network Manager

The Network Manager is responsible for identifying and recommending:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That appropriate filters and monitoring systems are in place, passing relevant information on to Safeguarding and Wellbeing Team where necessary.
- That the school meets the online safety technical requirements outlined in the school policies.
- Users may only access the school's networks through a properly enforced password protection scheme.
- The School Director and Senior Leaders are informed of any breaches in the processing of personal data.
- The School Director and Senior Leaders are informed of any suspicions of students who may be becoming radicalised

Roles and Responsibilities – Teaching and Support Staff

All staff receive online safety training and understand their responsibilities, as outlined in this policy. An audit of the online safety training needs of all staff will be carried out regularly. Training will be offered as a planned programme of formal online safety training available to all staff. All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable User Agreements. The school ensures that all staff receive regular updated online safety training, at least every two years.

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school's Online Safety Policy.
- They have read, understood, and signed the relevant Staff Internet Acceptable User Agreement as well as other related policies such as the Staff Behaviour (Code of Conduct) and Child Protection and Safeguarding policies.
- They report any suspected misuse or problem to the SDSL/School Director/Chair of Trustees as appropriate for investigation/action/sanction.
- They report any suspected breach of processing any personal data to the School Director and/or Data Protection Officer/Chair of Trustees.
- Digital communications with students, which are conducted through Microsoft 365, are on a professional level in line with the Staff Behaviour (Code of Conduct) Policy, and only carried out using official school systems.
- Students understand and follow the school's Online Safety Policy and the Student Internet Acceptable User Agreement.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons and in extra-curricular and extended school activities.
- They are 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.
- They are aware of the online safety issues pertaining to electronic communication and social media usage.
- They are alert to, and report to the School Director and/or DSL, any suspicions of students who may be becoming radicalised.
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Roles and Responsibilities – Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

- Parents and carers will be responsible for endorsing (by signature) the Student Internet Acceptable Use Agreement.

- Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will, therefore, take every opportunity to help parents/carers understand these issues through: − Sending information on internet safety and the importance of monitoring internet use at home to all parents/carers.

Online safety in the curriculum

Online safety is taught in specific areas of the curriculum but is also emphasised whenever students are using computers online. Staff always consider age-appropriateness when speaking of online safety and will be aware of those students who may be particularly vulnerable, e.g. looked after children or those with special needs. The school may use external resources and external visitors to assist in lessons, but appropriate members of staff will check in advance to ensure that they will enhance lessons and that materials used are appropriate for them.

Relationships and Sex Education

Students are taught about:

- Online safety and harm.
- Positive, healthy, and respectful relationships online.
- The effects of their online actions.
- How to recognise and show respectful behaviour online. Computing in the curriculum
- Principles of online safety.
- Where to obtain help and support if they are concerned about any online content or contact.

Computing in the curriculum

- Principles of online safety.
- Where to obtain help and support if they are concerned about any online content or contact.

Life Skills in the curriculum

- Media literacy online.
- Distinguishing fact from fiction online.

Online safety throughout the curriculum

Key online safety messages will be reinforced as part of a planned programme of personal development, including:

- How to evaluate what they see online – to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- How to recognise persuasion techniques.
- How to recognise acceptable and unacceptable online behaviour – to understand the need for the acceptable computer usage agreement and to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside school.
- How to identify online risks.

- How and when to seek support.
- To recognise how their data is taken and used from them daily across all their devices and how it is in their best interests to maintain a positive digital presence.
- To understand that free services are seldom ‘free’ and evaluate if these are services, they want to use at all.
- The need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet. Where students are allowed to search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the students visit.

It is accepted that from time-to-time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being flagged. In such a situation, staff should notify the Network Manager that this is happening so that any safeguarding alerts will not be escalated.

Management of infrastructure

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people will be effective in carrying out their online safety responsibilities:

- Personal data is held and processed in compliance with the Data Protection Act and GDPR. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Servers, wireless systems, and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems appropriate to their role. Access rights available to groups of users are given and monitored by the Network Manager. These will be reviewed, at least annually with the SLT.
- Access to areas where data is stored will only be granted to those with a valid reason to do so. Access to sensitive areas will only be given after being granted permission by the School Director.
- All users will be provided with a username and password by the Network Manager.
- In the event of a serious security incident, the police may request, and will be allowed access to, passwords used for encryption.
- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Any filtering issues should be reported immediately to the Network Manager.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- Only Northleigh House School employees are allowed to use school owned laptops and/or any other school owned devices that may be used out of school, e.g. school mobile phones
- The school infrastructure and individual workstations are protected by up-to-date virus software.

Protocols on using digital and video images

- When using digital images, staff inform and educate students about the risks associated with taking, using, sharing, publishing, and distributing images. They recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- If any incidents come to light about 'sexting', i.e. the sharing of sexual images of students under the age of 18, the Designated Safeguarding Lead should be advised in the first instance.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Staff and Students are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Permissions for the use of images is coordinated by our Compliance Officer. Staff should check permissions before distributing photos. Any images should only be stored on school equipment. Personal equipment, if used, should only store images for as long as is necessary to capture and then upload to the school systems, it should then be promptly deleted from the personal device.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained, and the student where appropriate.

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act and in compliance with the General Data Protection Regulation which state that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant, and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff will ensure that they comply with our Information Security Policy by:
- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Using personal data only on secure password protected computers and other devices and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.
- Laptops/PC's should be locked if left unattended.

Protocols for handling electronic communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users will be expected to know and understand school policies on email, teams chat, social media (and other relevant electronic devices protocols).
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email or Teams communications that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email or teams chat but must follow the procedures in the Staff Behaviour (Code of Conduct) Policy, Staff Internet Acceptable Use Agreement and Student Internet Acceptable Use Agreement.
- The school operates a CCTV system and recordings are kept for 30 days to ensure the safety and wellbeing, access to the footage is password protected.
- Any digital communication between staff and students or parents/carers (email, teams chat etc) must be professional in tone and content.

Unsuitable/inappropriate activities

Certain activities are referred to in the Acceptable Computer Usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and online safety must be followed if any apparent, suspected, or actual misuse appears to involve illegal or inappropriate activities, such as:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity, or materials.
- Potential radicalisation of students.

Should any serious online safety incidents take place, the appropriate external authorities will be informed, e.g. Local Authority Designated Officer (LADO), police etc or, for personal data breaches, the Information Commissioner's Office (ICO).

Review Date: September 2024