HIGHDOWN SCHOOL AND SIXTH FORM CENTRE

ONLINE SAFETY POLICY

Aspiration – Respect – Excellence

Monitoring, Evaluation and Review

Author	Mr M A Grantham [Head of School]	Review Period	3 years
Version	2.1	Status	Approved
Committee	Learning and Teaching	Date Approved	18th October 2022 [Amended June 2023]
Link Governor	Dr C Foulkes	Review Date	October 2025

HIGHDOWN SCHOOL AND SIXTH FORM CENTRE
ONLINE SAFETY POLICY

This policy should be read in conjunction with the following policies:

- Behaviour Policy
- Antibullying and Discrimination Policy
- Safeguarding and Child Protection Policy
- Bring Your Own Device [BYOD] Policy
- PSHCE (including RSE) Policy
- Data Protection Policy

Introduction

New technologies have become integral to the lives of young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe Internet access at all times. The requirement to ensure that young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This policy will help to ensure safe and appropriate use. The use of the exciting and innovative tools in lessons and at home has the potential to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The academy provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. This policy explains how the academy intends

to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

This policy applies to all members of the Highdown community (including staff, students, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of our academy ICT systems, both in and out of Highdown School.

Aims and objectives

- To establish the 'ground rules' we have for using ICT equipment and the Internet
- To ensure safe and appropriate use of the internet and related communication technologies
- To use ICT to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the academy's management information systems
- To create an environment in which staff use ICT confidently in their work and students use their ICT skills confidently to enhance their learning

Roles and responsibilities

This section outlines the roles and responsibilities for online safety of individuals and groups within the school.

(i) Governors

The Governors Learning and Teaching committee is responsible for the approval of this policy and for reviewing the effectiveness of the policy. This will be through meetings between the Link Curriculum Governor and Link Safeguarding Governor and the Deputy Head [Curriculum and Professional Learning] and Designated Safeguarding Lead, respectively, with reports back the Learning and Teaching Committee. Governors must ensure that appropriate filtering and monitoring systems are in place[1].

(ii) Senior Leaders

The Headteacher and Head of School are responsible for ensuring:

- The safety (including online safety) of all members of the academy community, although the day-to-day responsibility for online safety may be delegated to the Designated Safeguarding Lead
- Adequate training is provided
- Effective filtering and monitoring systems are in place
- That relevant procedures in the event of an online safety allegation are known and understood
- Establishing and reviewing the online safety policy and documents (in conjunction with Designated Safeguarding Lead), including filtering and monitoring systems

[1] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

(iii) Designated Safeguarding Lead

The academy's Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

With the teacher responsible for ICT across the curriculum, the Designated Safeguarding Lead takes day to day responsibility for online safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff, Safeguarding Governor and Senior Leaders on all issues related to online safety
- Ensuring that all staff are aware of the procedures that need to be followed should they be concerned about an online safety issue or breach of Online Safety policy and protocols
- Providing training and advice for staff
- Receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Coordinating and reviewing online safety education programme at Highdown School
- Signposting resources for parents/carers and staff, e.g. on the Academy website, [See Appendix 1]
- Reviewing existing systems and processes to support online safety, e.g. SWGfL 360˚ audit
- Understanding the filtering and monitoring systems and processes in place

(iv) Network Manager

The Network Manager is responsible for ensuring that:

- The academy's ICT infrastructure is secure and meets online safety technical requirements and is not open to misuse or malicious attacks
- The academy's filtering and monitoring systems are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. These must be reviewed at least annually, with the senior leader with responsibility for whole school IT, who will report to the DSL and Governing Body.
- Network Manager keeps up to date with online safety technical information
- The use of the academy's ICT infrastructure (network, remote access, e-mail, etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Safeguarding Lead and/or senior leaders for investigation/action/sanction

(v) Teaching & Support Staff

All teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current academy Online Safety policy and practices, including an understanding of filtering and monitoring systems
- Online safety issues are embedded in all aspects of the curriculum and other academy activities
- Students understand and follow the online safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended curriculum activities
- 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

(vi) Students (to an age-appropriate level)

- Are responsible for using the academy ICT systems in accordance with the Acceptable Usage Policy, which they will be required to sign before being given access to academy systems. Parents/carers will be required to read through and sign alongside their child's signature
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety policy also covers their actions out of school, if related to their membership of Highdown School.

(vii) 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. 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. Highdown School will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Usage Policy
- Accessing our website in accordance with the relevant Acceptable Usage Policy

(viii) Community Users

Community Users who access Highdown's ICT systems/website as part of extended provision will be expected to sign a Volunteer User AUP before being provided with access to IT systems.

Curriculum and learning

Online safety education is provided as part of the planned PSHCE and ICT and Computing curricula, including assemblies and Safer Internet Day activities.

- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information
- Students will be made aware of the following considerations relating to online safety:
    - SMART:
        - Safe: keep safe and do not give our personal information
        - Meeting: don't arrange to meet strangers you have met online by yourself
        - Accepting: don't accept unsolicited online requests, emails, files
        - Reliable: make sure websites used and information retrieved are reliable
        - Tell your parent/carer or trusted adult if someone or something makes you feel uncomfortable or worried online
    - 4Cs:
        - Content: what you access, download, share and post online
        - Contact: who you contact, meet and chat with online
        - Conduct: how you conduct and behave yourself online
        - Commerce: how you protect yourself against online scams
- Students will be taught how to evaluate Internet content:
    - We will ensure that the use of Internet-derived materials by staff and by students complies

with copyright law
    - Students will be advised never to give out personal details of any kind which may identify them, their friends or their location
    - Students will be made aware of how they can report abuse and who they should report abuse to
    - Students will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future
    - Students will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others
- Highdown School will educate stakeholders in the safe use of social media, including Facebook, Twitter, Snapchat and Instagram
- Students are helped to understand the need for the AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of Highdown School
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for the use of ICT systems and the Internet are shared with students
- Staff must act as good role models in their use of ICT
- Websites:
    - 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
    - Staff will preview any recommended sites before use
    - "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information
    - If Internet research is set for home learning, specific sites should be suggested that have previously been checked by staff. Parents will be advised to supervise any further research.
    - All users must observe copyright of materials published on the Internet
    - Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at Highdown School is tracked and logged
    - Highdown School only allows the Designated Safeguarding Lead, Network Manager and SLT to access to Internet logs
- Social Media:
    - Students are taught about the dangers of social media and potential risks of grooming for CSE or radicalisation
    - Students are taught about how to keep safe when using social media within the Computing/ICT curriculum and PSHCE Curriculum
    - Students will be taught, as part of the PSHCE curriculum, about the law in connection with social media and creating/sharing images.
- Managing emerging technologies:
    - Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
    - Technologies, such as mobile phones, with wireless Internet access can bypass filtering systems and present a new route to undesirable material and communications. Student laptops must only connect to the BYOD network and should not be tethered to a mobile device to avoid security and safeguarding systems. Highdown will monitor this and continue to review this potential issue

- The sending of abusive or inappropriate messages is forbidden

- Bring Your Own Device (BYOD):
  - The primary purpose of all mobile/personal devices in school is educational.
  - The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software, and online services become available for learning and teaching, within and beyond the classroom. Highdown School is implementing a BYOD policy from Setpember 2022 starting with Years 7 and 8 and phasing in with each new Year 7 intake. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations have included levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing, and monitoring. This list is not exhaustive, and a BYOD policy has been published.
    - The academy will have a set of clear expectations and responsibilities for all users
    - The school adheres to the Data Protection Act principles
    - All users are provided with and accept the Acceptable Use Agreement and Personal Laptop Acceptable Use Agreement
    - All network systems are secure and access for users is differentiated
    - Where possible these devices will be covered by the normal filtering systems, while being used on the premises
    - All users will use their username and password and keep this safe
    - Training will be provided for staff and students to support BYOD
    - Regular audits and monitoring of usage will take place to ensure compliance
    - Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
  - To reduce the potential for misuse of mobile phone devices, students will not be allowed to use these in indoor spaces within the academy, nor in lessons unless permission is given by the class teacher where it is required to support learning.

Safeguarding

- Highdown School is fully committed to safeguarding and promoting the welfare of all its students. Every member of staff recognises that safeguarding against radicalisation, extremism and CSE is no different to safeguarding against any other vulnerability in today's society
- We take reasonable measures to protect students from the risk of radicalisation and CSE, for example by using filters on the internet and monitoring systems
- Our Safeguarding and Online Safety policies set out our beliefs, strategies, and procedures to protect vulnerable individuals from being radicalised, or exposed to extremist views or potential CSE, by identifying who they are and promptly providing them with support.
- The PSHCE curriculum and ICT/Computing curriculum will promote responsible use of online media, including social networking sites, by students so that they do not become engaged in online child on child abuse (i.e. cyberbullying) and that they know how to keep safe in a digital world. Students will also learn about a wide range of other online risks, including:
  - Unsafe communications:
    - Online relationships
    - Fake profiles
    - Cyber-bullying
    - Grooming
    - CSE
    - Sexting/Sharing nudes and/or semi-nudes

- Online information:
    - Online reputation
    - Age-inappropriate content
    - Online fraud
    - Fake news and hoaxes
    - Personal data
    - Dark Web
- Effects on health, wellbeing and lifestyle:
    - Online vs offline identity
    - Social media and mental health
    - Device addiction
    - Online (viral) challenges
    - Online gambling
    - Radicalisation

- All staff and every parent/carer of a student at Highdown School has unlimited access to National Online Safety portal from the National College. This provides a wide range of guides, webinars, courses and information to promote online safety, with parents and staff working together to support young people develop as positive and responsible digital citizens.

Incidents of misuse

Any online safety incidents must immediately be reported to the Headteacher or Head of School (if relating to a member of staff) or the Designated Safeguarding Lead (if relating to a student) who will investigate further following e-safety and safeguarding policies and guidance.

It is hoped that all members of the Highdown community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Highdown community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Monitoring, evaluation and review

The Online Safety Policy will be reviewed annually by the Designated Safeguarding Lead in conjunction with the Network Manager and Link Curriculum and Safeguarding Governors and will be reported on to the Governors Learning and Teaching Committee.

Appendix 1: Online resources to support online safety

NSPCC Online Safety Information

UK Safer Internet Centre (UKSIC)

Childnet: advice for parents to talk their child about online issues

Childnet's Parent and Carer Toolkit: advice for parents/carers for supporting children of different ages with a range of key online safety topics

Internet Watch Foundation (IWF): hotline for reporting images and videos of child sexual abuse online.

South West Grid for Learning (SWGfL): advice and resources to support use of Internet technologies safely

BBC Own It: articles and advice to help young people be the boss of their online lives

ThinkUKnow: provides information for young people and parents and a reporting tool for children to report sexual abuse and grooming

Report Harmful Content: gives advice on how to report online problems, including harmful content

Report Remove Tool: to report to remove a nude image or video shared online

YoungMinds: to get advice about wellbeing and mental health of young people

Internet Matters: support and advice across a range of online safety issues, including useful guides for setting parental controls