HEANOR GATE
SPENCER ACADEMY

ICT, Online Safety & Social Media Use Policy

2025-26

SPENCER
ACADEMIES TRUST

Contents

1. Aims

Our school aims are to:

- Ensure the online safety of pupils, staff, volunteers and Governors.
- Strengthen whole school awareness of any significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.
- Implementation and development monitored by the IT Lead annually in the summer term and reported to the Executive Principal.
- Serious online safety incidents are notified to the IT lead in the first instance and, if appropriate escalation is decided, to the designated Safeguarding Lead, the Executive Principal and/or Police.
- Reviewed annually or in light of significant changes, threats or developments to online safety.

2. Our Approach to Online Safety

Heanor Gate Spencer Academy believes that it is everyone's responsibility within the school community to be confident and competent in the use of technology and how to engage safely in the online world. We therefore aim to strengthen this area through education and training. This education takes place through a variety of routes including PSHE and Computing lessons, assemblies and one-off events led by specialist providers. Resources from outside bodies, like CEOPS and NSPCC, are used as well to support internally produced resources.

The highest standards of behaviour and mature, responsible, considerate attitudes are expected of pupils and staff in school and it is important that these aims are applied to their use of technology. We believe that the benefits offered by use of the internet far outweigh the problems caused by abuse, and that every aspect of digital technology can have educational value.

Pupils are taught to appreciate that the internet is a public place and that everything they do online leaves a footprint which may be seen by those they meet, now and in later life. Throughout all Key Stages we encourage our pupils to exercise care and due diligence when selecting to engage with all forms of communication online. We promote the use of

maximum privacy settings and that every individual is responsible to ensure that their online presence is maintained in a positive light and encouraged to be cautious in their treatment of people and organisations they communicate with.

Although the school internet system is protected by internal and external filtering, pupils are made aware that this is never totally effective and that they are responsible for reporting to a member of staff issues where undesirable material can be accessed.

Pupils are made aware of the legal restrictions surrounding online behaviour. They are informed of the sources of support, both within and outside bodies, available to deal with any problems which may occur, including cyber-bullying, online grooming and radicalisation. All instances of misbehaviour online are dealt with in-line with the school discipline and behaviour policies.

3. Development/Monitoring/Review of this Policy

This IT & Online Safety Policy has been developed by the following leads in school:

- Assistant Principal & Designated Safeguarding Lead - Mrs M Britton
- Assistant Principal - Standard & Expectations - Mr Julian Wright
- IT Lead & CTL for Computing & Business - Mr J Chambers
- Computing Teachers: Mr S Nadin, Mr T Cornall, Mr S Brown and Mr J Hornsby
- IT Technicians - Mr L Reid and Miss S McCleod

4. Roles and Responsibilities

Governors

Governors are responsible for the approval of the IT & Online Safety Policy and for reviewing its effectiveness of the policy. They are to monitor and hold the Executive Principal to account for its implementation.

Executive Principal and Senior Leadership Team

The DSL is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety filtering will be delegated to the IT Lead and Assistant Principal - Standards & Expectations.

IT Lead

The IT Lead is responsible for:

- Ensuring the scrutiny of day to day online safety.
- Playing an active role in establishing and reviewing the school online safety policies.
- Creating an E-Safety curriculum which is taught to all students in Key Stage 3 as part of their Computing programmes of study. Students will receive 5-6 hours of lessons at the start of each year (in Key Stage 3) tailored on E-Safety needs of the individual year group.
- Organising an IT & Online Safety Review once a year to ascertain key points raised during the teaching of E-Safety and also to discuss any pastoral issues raised throughout the year which may inform changes to the following year's curriculum.

- Providing training where required to staff members on key E-Safety issues.
- Reporting on request to the Senior Leadership Team.

IT Technician Team

The IT Technician team are responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required IT safety standards and requirements.
- The users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis.
- The use of network/email/Google activity access is logged so the IT Lead can investigate any individual for potential disciplinary action.
- The monitoring systems are implemented, updated and fit for purpose.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school IT & Online Safety Policy and practices.
- They have read and understood the staff Responsible Use Policy (RUP).
- They report any suspected misuse or problem to the IT Lead for investigation.
- All digital communications with students/parents/guardians should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded into relevant aspects of the curriculum and other activities students understand and follow the IT & Online Safety Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Where necessary staff and pupils should report unsuitable material found during internet searches to network services so that the filtering system can be fine-tuned.

Designated Safeguarding Lead

This person is trained in IT & Online Safety issues and is aware of the potential for safeguarding issues that may arise from:

- Sharing of personal data
- Access to illegal/inappropriate content (or material)
- Inappropriate online contact with adults/strangers
- Potential incidents of grooming and cyber-bullying

IT & Online Safety Policy Leads

The Online Safety Committee provides a consultative group that has a wide representation from within the school body. It has responsibility for issues regarding Online Safety, for monitoring the IT & Online Safety Policy and for analysing the impact of initiatives. Members of the Online Safety Committee will work collaboratively on the following:

- The production/review/monitoring of the effectiveness of the school Online Safety Policy.
- Mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression through the PSHE programme consulting stakeholders – including parents/guardians and the students about the online safety provision.
- Monitoring the implementation of improvement actions identified through use of the 360degree safe self-review tool.

Pupils

- Pupils are responsible for using the school systems in accordance with the Responsible Use and IT & Online Safety Policy.
- They need to understand the importance of reporting abuse, misuse or access to inappropriate material to a member of staff as soon as possible
- They should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's IT & Online Safety policy covers their actions out of school.

Parents/Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use digital technologies in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, and the school website and encourage them to support the school in promoting good online safety practice. Parents/Guardians are also clear that they are fully responsible for any misuse which occurs on their premises and clear that this could lead to further disciplinary action for those found involved upon investigations led by the IT Lead or Associate Assistant Principal - Standard & Expectations.

5. Online Safety Contacts & References

- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- Childline: www.childline.org.uk
- Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
- Cybermentors: www.cybermentors.org.uk
- Digizen: www.digizen.org.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Kidsmart: www.kidsmart.org.uk
- Think U Know website: www.thinkuknow.co.uk
- Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

6. Remote Learning

All staff who interact with children and young people, including online, will continue to look out for signs a child may be at risk. Online teaching should follow usual principles for safe and acceptable use of technology.

Google Classroom is the online learning platform that is used by the school. This platform allows work to be set, completed and marked effectively whilst minimising any online safeguarding risk.

Online communication with students is done through regulated platforms (school email, google classroom). Staff will receive basic training in how to use Google Classroom.

In certain, rare circumstances staff may need to utilise video conferencing. In these circumstances, permission must be granted by the IT Lead who will also provide support and guidance.

7. Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The Designated Safeguarding Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

8. Social Media Use

Staff

All staff who engage with social media in or outside of school must:

- Be responsible and respectful users and should be conscious at all times of the need to keep their personal and professional/school lives separate.
- Seek permission by the Senior Leadership Team to authorise work related posts from a personal social media account.
- Where possible use faculty/pastoral linked social media accounts for marketing and educational purposes. Usernames & passwords should be logged with the IT Lead.
- Not put themselves in a position where there is a conflict between the school and their personal interests.
- Not engage in activities on social media which may bring Heanor Gate Spencer Academy's reputation into disrepute.
- Not represent their personal views as those of Heanor Gate Spencer Academy on any social medium, work or personal.
- Not discuss personal information about other pupils, Heanor Gate Spencer Academy and the wider community they interact with on any social media platforms.
- Not use social media and the internet in any way to attack, insult, abuse or defame pupils, pupils' family members, colleagues, other professionals, other organisations or Heanor Gate Spencer Academy.
- Ensure that their personal use of social media platforms should not identify themselves as members of Heanor Gate Spencer Academy in their personal profiles, unless specifically linked to an approved job role within the school community where it serves a purpose to professionally market the school. This is to prevent information

being linked with the school and to safeguard the privacy of staff members, pupils and parents and the wider school community. Line Managers may request deletion of posts/material which is deemed inappropriate and detrimental to the school image.

- Not have contact through any personal social media platforms with any pupil, whether from Heanor Gate Spencer Academy or any other school, other than those social media accounts approved by the Senior Leadership Team or the IT Lead, unless the staff concerned are family members.
- Not redistribute/post photographs, videos or any other types of images of pupils and their families or images depicting staff members, clothing with school logos or images identifying school premises on personal or public web space without prior permission from the school.
- Not to use school email addresses for setting up personal social media accounts or to communicate through such media without appropriate permission from their Line Manager.
- Not edit open access online encyclopedias such as Wikipedia in a personal capacity. The source of the correction will be recorded and Heanor Gate Spencer Academy reserves the right to amend these details for their sole purpose and where necessary follow disciplinary proceedings against the staff who acted in their personal capacity without Senior Leadership Team approval.
- Ensure that they set the privacy levels of their personal social media accounts as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
- Ensure passwords are confidential and changed often.

Breaches to the guidelines above may result in legal action, disciplinary action or sanctions in line with the published school policies for staff.

Parents/Guardians

Although social networking platforms may appear to be the quickest and easiest way to express frustrations or concerns, it is rarely appropriate to do so. Instead, the school encourages a transparent and open dialogue between staff, students and parents through the use of constructive confidential channels through the arrangement of a meeting, a phone call or a clear email of the issue concerned.

The school considers the following examples to be inappropriate uses of social networking sites:

- Making allegations about other pupils
- Making complaints about staff
- Posting negative/offensive comments about specific pupils/staff
- Posting racist comments
- Posting comments which encourage violence

The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step, the school will usually discuss the matter with the parent to try and resolve the matter and to ask that the relevant information be removed from the social networking platform in question. If the parent refuses to do this and continues to use social networking platform in a manner

Heanor Gate Spencer Academy considers inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstance warrants this.
- Set out the school's concerns to you in writing, giving you a warning and requesting that the material in question is removed.
- Contact the Police where the school feels it appropriate – for example, if it considers crime (such as harassment) has been committed; or in cases where the posting has a racial or homophobic element, is considered to be grossly obscene or is threatening violence.
- Take other legal action against the individual.

Where parents or pupils are found to have breached this policy the Executive Principal, Associate Assistant Principal - Standard & Expectations and IT Lead and will meet with parents to remind them of this policy. Following this meeting a decision is made as to what further course of action which may be taken as a result to damage to the school, individuals or the school's reputation.

9. Use of Artificial Intelligence (AI)

The school acknowledges the increasing role of Artificial Intelligence (AI) in education and social media. AI tools can offer valuable learning and teaching opportunities but must be used responsibly to ensure safety, privacy, and fairness.

Student Use of AI

- Educational Purposes Only: Students may only use AI tools (e.g., chatbots, language models, image generators) when approved by teaching staff and for specific educational activities.
- Some online Artificial Intelligence tools are not accessible through our computer network.
- Misuse Prohibited: Using AI to produce inappropriate content, plagiarise, impersonate others, or bypass assessments is strictly forbidden and may result in disciplinary action.
- Digital Literacy: The school will provide guidance to students on the ethical use of AI, including recognising bias, understanding misinformation, and using AI safely and responsibly.
- Privacy and Consent: Students should not input personal data or confidential information into AI platforms unless explicitly instructed to do so under secure conditions.

Staff Use of AI

- Professional Use: Staff may use AI tools to support teaching, assessment, planning, and communication, provided they uphold data protection and professional standards.
- Safeguarding Responsibilities: AI must not be used to replace professional judgement in areas involving student welfare, behaviour, or safeguarding.
- Data Protection: Staff must ensure any AI tools used are compliant with UK GDPR. Tools that process personal or sensitive data should be reviewed and approved by the school's data protection lead.

- Training and Oversight: Staff will receive training on the appropriate use of AI in educational contexts, with ongoing review to ensure safe and effective practice.

Monitoring and Oversight

- The school may use AI-based monitoring systems to help identify harmful online activity or risks to pupil safety on school devices or networks.
- Any AI system used will be reviewed regularly for accuracy, fairness, and alignment with safeguarding and privacy standards.

10. School's Response to Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Spencer Academy Trust staff expectations and Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

School staff have specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, tablets and other electronic devices, where they believe there is 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm
- Disrupt teaching
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material
- Retain it as evidence (of a criminal offence or a breach of school discipline) - Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

11. Related Policies

- Behaviour Policy
- Exclusion Policy
- Child Protection & Safeguarding Policy

Appendix 1: Pupils and Parents/Guardians Responsible Use Policy (RUP)

Pupils and parents/guardians will read and follow the rules in the acceptable use code of conduct as outlined below.

When pupils and parents/carers use the school's IT systems they will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep their username and passwords safe and not share with others
- Keep private information safe at all times and not give their name, address or telephone number to anyone without the permission of the teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if they find any material which might cause them or others upset, distress or harm
- Always log off or shut down a computer when they have finished working on it.

They will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting a parent/carer, or without adult supervision
- Pupils will be aware that the school will monitor the websites they visit and that there will be consequences if they don't follow the rules.
- Parents/carers will support the school in ensuring their child understands and adheres to these conditions
- Use social media platforms to bring the school, staff or other pupils reputation into disrepute.

Appendix 2: Staff, Governors, Volunteers and Visitors Responsible Use Policy (RUP)

When using the school's IT systems and accessing the internet in school, or outside school on a work device staff will:

- Not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Not use them in any way which could harm the school's reputation
- Not use any improper language when communicating online, including in emails or other messaging services
- Not install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Not share passwords with others or log in to the school's network using someone else's details
- Not take photographs of pupils without checking with their Line Manager first
- Not share confidential information about the school, its pupils or staff, or other members of the community
- Not access, modify or share data they are not authorised to access, modify or share
- Not promote private businesses, unless that business is directly related to the school
- Only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of their role
- Be aware that the school will monitor the websites they visit and their use of the school's IT facilities and systems.
- Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- Let the Designated Safeguarding Lead (DSL) and IT Lead know if a pupil informs them they have found any material which might upset, distress or harm them or others.
- Staff will also take the same steps if they themselves find any material which might upset, distress or harm them or others.
- Always use the school's IT systems and internet responsibly, and ensure that pupils in their care do so too.