Hamilton School

An honest school that strives to do the best.

Online safety policy

All of the students at Hamilton School have Autistic Spectrum Disorders; they have greater difficulty than other students with social understanding and communication. It is therefore essential that this policy be implemented to support all students.

Young people with Autism and other communication difficulties often find internet communication easier than face to face communication. On the internet people's use of consistent and easily recognisable emoticons replaces the need to decode people's body language, facial expressions and vocal tone that can be problematic in personal communications.

Internet-learning provides opportunities for learning through repetition that supports students who take longer to learn new things and embeds the learning they do in the classroom by undertaking activities as many times as they need to in order to consolidate their learning.

Alongside the many benefits to young people there are also a number of risks. With access to technology comes the potential for cyberbullying, online grooming and risk of exposure to inappropriate content. This is a risk for all young people using the internet but the risk can be more profound for young people with ASD as a result of increased vulnerability, tendencies towards obsessive compulsive behaviour and social naivety.

For this reason, the requirement to ensure that students and young people are able to use the internet and related communications technologies appropriately and safely needs to be addressed as part of the wider duty of care to which all who work in schools are bound. This online safety policy has been developed to help ensure safe and appropriate use of ICT. The development and implementation of this policy should involve all the stakeholders in a young person's education from the Head Teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

1. Introduction

1.1 As stated in Keeping Children Safe in Education (2024), the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content

- being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact

- being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct

- online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non- consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce

- risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

1.2 The governing body of Hamilton School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.3 This policy was adopted by the governing body on *_10 April 2025_ and will be reviewed annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

1.4 At Hamilton School we recognise the importance of Online safety for all students. This policy outlines our commitment to ensuring a safe and responsible use of technology and the internet for our students. We aim to empower them with the knowledge and skills to navigate the digital world safely and confidently.

2. Basic principles

2.1 In adopting this policy, the governing body has taken into account the expectations set out in *Keeping Children Safe in Education (2024)* and by Ofsted, which state that rigorous and regularly updated online safety policies and procedures should be in place. These policies should be written in plain English, with contributions from the whole school community, updated regularly, and ratified by governors.

2.2 This policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors, and community users who have access to or use the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing body expects the Head Teacher to ensure that this policy is Training in Online safety must be given high priority across the school, with regular reviews to reflect emerging risks. Consultation on the arrangements for Online safety should be ongoing, involving all employees and stakeholders, and necessary amendments to this policy should be submitted to the governing body for approval.

2.4 The principal context for this policy is the school's duty to safeguard children in line with *Keeping Children Safe in Education (2024)*. This policy forms part of the school's wider safeguarding approach and should be applied alongside:

- The school's Child Protection and Safeguarding Policy,
- Procedures set by the Birmingham Safeguarding Children Board,
- The school's Behaviour Policy,
- The school's Anti-Bullying Policy, and
- The rules and procedures governing the conduct of employees.

2.5 The governing body expects the Head Teacher to arrange for this policy to be published and shared with all employees and volunteers in the school. Additionally, clear guidance and training on acceptable use should be provided to all staff, and age-appropriate instruction on Online safety should be embedded into the curriculum and pastoral support to ensure that pupils understand how to stay safe online.

3. Roles and responsibilities

Governing body

3.1 The governing body will consider and ratify this Online safety policy, and review it annually in the light of guidance from the Local Authority, or sooner if the Local Authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in Online safety training if they use information and communication technology in their capacity as school governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head Teacher

3.3 The Head Teacher is responsible for ensuring that

- the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this online safety policy;
- the governing body is given necessary advice on securing appropriate information and communication technology systems;
- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
- the school has a designated member of the Senior Leadership Team (Gabriella Fokti) to co-ordinate Online safety and that this person has adequate support from, and provides support to, other employees, particularly other members of the safeguarding team.
- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all employees with training in Online safety relevant to their roles and responsibilities and that training is also provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors, as the case may be;
- pupils are taught Online safety as an essential part of the curriculum;
- the Senior Leadership Team is aware of the procedures to be followed in the event of a serious Online safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem;
- records are kept of all Online safety incidents and that these are reported to the designated member of the Senior Leadership Team;
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Network Manager

3.4 The Network Manager is responsible for:

- Ensuring that any Online safety related issues that arise are reported to the designated member of the Senior Leadership Team (Gabriella Fokti).
- Ensuring that users can only access the school's networks through an authorised and password-protected system, with passwords regularly changed.
- Ensuring that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date).
- Ensuring that the school's ICT systems are secure.

- Ensuring that access control and encryption are in place to protect personal and sensitive information held on school-owned devices.
- Ensuring that filtering and monitoring processes are rigorous and up to date.
- Ensuring that the use of the network, remote access, and email is regularly monitored so that any misuse, or attempted misuse, can be reported to the designated member of the Senior Leadership Team or the Head Teacher for investigation.
- Ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keeping up to date with the school's Online safety policy and relevant technical developments in order to effectively carry out their role and to inform and update others as needed.
- Maintaining up-to-date documentation of the school's e-security systems and technical procedures.
- Ensuring that all data held on students on school office machines is protected with appropriate access controls.

Teachers

3.5 Teachers are responsible for

- Teaching the online safety aspect of the computing curriculum within every lesson, adapting it to meet the individual needs of the pupils.
- Embedding broader Online safety principles into all relevant areas of the curriculum and other school activities, where appropriate.
- Supervising and guiding pupils carefully when they are engaged in learning activities involving online technology.
- Where appropriate, ensuring that pupils are aware of safe research practices and legal considerations relating to digital content, such as copyright, plagiarism, and responsible sharing.

All staff

3.6 All staff are responsible for

- Undertaking responsibilities as delegated by the Head Teacher, in line with their job descriptions and salary grade.
- Participating in Online safety training provided by the school and contributing to consultations about this policy and its application, including how Online safety is embedded within the curriculum.
- Using information and communication technology in accordance with this policy and the training provided.
- Reporting any suspected misuse, breaches, or concerns to the designated member of the Senior Leadership Team responsible for Online safety (Gabriella Fokti).
- Modelling safe, responsible, and professional behaviours in their use of technology.

- Ensuring that all digital communications with pupils remain professional and are conducted only through school-based systems, never through personal accounts or devices.
- Supporting pupils to follow the school's expectations around mobile phone use, including guiding them to put personal devices away in their bags if seen using them during the school day.

Students

3.7 Expectations on students should be as follows:

- Students are expected to use the school's information and communication technology systems and devices responsibly, in line with how they have been taught, the school's behaviour policy, and staff guidance.
- Access to the internet will always be supervised and monitored while on school premises.
- Students will only be granted access to age-appropriate and educational websites and applications, based on individual needs and risk assessments.
- Students who bring personal devices (e.g. mobile phones or tablets) to school — for example, for use on transport — are expected to keep them in their bags during the school day. Use of personal devices is subject to approval and monitoring by staff.
- Social media use and online communication will be closely monitored, with a strong focus on teaching pupils safe, respectful, and appropriate interaction skills both online and offline.

Other users

3.8 Volunteers, including governors, who support the school and use its information and communication technology systems and devices are expected to:

- Participate in Online safety training provided by the school, and engage in consultations about this policy and its application, including the role of Online safety within the curriculum.
- Use information and communication technology in line with this policy and the training they have received.
- Report any suspected misuse, breaches, or concerns to the designated member of the Senior Leadership Team responsible for Online safety (Gabriella Fokti)

Parents

3.9 Parents who help in the school as volunteers are covered by the expectations outlined in section 3.8 above.

- Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.
- The school recognises the important role that parents and carers play in supporting Online safety at home. We are committed to working in partnership with families to promote safe and responsible technology use beyond the school environment.

4. Acceptable use

4.1 The use of information and communication technology at Hamilton School should follow these general principles:

- This policy applies regardless of whether systems are being used on or off school premises, including remote access or home-based working.
- The school's ICT systems are intended primarily for educational use and for the management and administration of the school. During breaks, appropriate and reasonable personal use is permitted.
- All use of ICT must comply with Data Protection legislation and the school's Data Protection Policy.
- Users must not attempt to use the school's systems for any illegal activities or access to illegal material.
- Users must always communicate in a respectful, professional manner, whether communicating with pupils, colleagues, or external individuals.
- Users must not disclose their password to anyone and should not write it down or store it in a location where it could be accessed by others. Attempting to use another person's username or password is strictly prohibited.
- Users must report, as soon as possible, any illegal, inappropriate, or harmful material or activity to the designated member of the Senior Leadership Team responsible for Online safety (Gabriella Fokti).

4.2 Employees, volunteers, and governors who use the school's ICT systems and devices are expected to:

- Not open, copy, remove, or alter another user's files without their express permission.
- Only take and/or publish images of others with their permission — and, in the case of pupils, only with parental or guardian consent.
- When recording or publishing images for educational purposes, avoid including names or other personal identifying information.
- Communicate with pupils and parents only through the school's official communication systems, and not share or publish personal contact details through those systems.
- If using personal devices for work (with school agreement), ensure those devices are secure, password-protected, and encrypted.
- Not access personal social networking sites via the school's ICT systems.

- Not open hyperlinks or attachments in emails unless the source is known and trusted.
- Ensure their data is backed up regularly in accordance with school ICT procedures.
- Only download or upload large quantities of data with permission, to avoid overloading the school's systems.
- Not install software or alter computer settings unless permitted under school ICT rules.
- Never deliberately disable, damage, or tamper with school ICT equipment.
- Report any damage, faults, or suspected security issues to the appropriate staff member immediately.

4.3 Use of social media platforms or networking sites — whether by pupils or employees — is subject to the same standards of behaviour and conduct that the school expects in all other contexts. These expectations are set out in the **school's Code of Conduct for Support Staff** and the **Teachers' Standards**.

The school recognises the separation between private life and professional responsibilities. However, it reserves the right to intervene where:

- There is evidence that the law may have been broken;
- An employee may be in breach of contract; or
- The reputation of the school may be, or has been, brought into disrepute.

All staff and pupils should be aware that online actions have real-world consequences and that the same standards of respect, professionalism, and safeguarding apply online as in school.

4.4 Guidelines for responsible and safe internet use will be communicated clearly and consistently.

4.5 Where appropriate, pupils will be actively encouraged to report any concerns related to online safety — including cyberbullying, exposure to inappropriate content, or online threats — to a trusted adult within the school. Staff will ensure pupils know how and where to seek help, and that they feel safe and supported in doing so.

5. Education and training

5.1 Education and training in Online safety will be given high priority across the school.

5.2 The education of pupils in online safety is an essential part of the school's online safety provision and will be included in all parts of the curriculum.

5.3 The school will offer education and information to parents, carers and community users of the school about online safety.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

5.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

6. Data Protection

6.1 The school will ensure that all use of its information and communication technology systems complies with current data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All users will be made aware of the school's Data Protection Policy, including the requirement for the secure handling, storage, and transmission of personal and sensitive information.

7. Technical aspects of online safety

7.1 The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

7.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

7.4 The school's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

7.6 Additional monitoring may be carried out where there is evidence of, or suspicion of, misuse or breach of policy, as part of a formal investigation.

8. Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection must be reported immediately, following the procedures set out by the Birmingham Safeguarding Children Partnership and the school's Child Protection and Safeguarding Policy.

8.2 Any suspicions of other illegal activity should be reported to the Head Teacher, who will seek advice from the appropriate agencies or professionals depending on the nature of the activity and individuals involved. Where appropriate, the Head Teacher will report the matter to the police and may initiate internal disciplinary procedures.

8.3 Suspected incidents of inappropriate – but not illegal – use of information and communication technology should be reported to the Head Teacher or the designated member of the Senior Leadership Team (currently Gabriella Fokti). These will be investigated appropriately and may result in:

- Informal management discussions
- Targeted support or training
- Disciplinary action in line with staff conduct procedures
- Behaviour support strategies in line with the school's Behaviour Policy for Pupils

9. Handling complaints:

9.1 The school will take all reasonable precautions to ensure the safety of users online. However, due to the international nature and constantly evolving landscape of internet content, and the widespread availability of mobile technologies, it is not possible to guarantee that all unsuitable material will be blocked or prevented from appearing on a school device. Therefore, the school, its internet service provider, and the Local Authority cannot accept liability for any content accessed or for the consequences of internet use.

9.2 All staff and pupils are made aware of what constitutes unacceptable use of ICT systems and the potential consequences. Where necessary, appropriate sanctions will be applied, which may include:

• A formal interview with the Head Teacher, Assistant Head Teacher (lead for Online safety), or a designated member of the Senior Leadership Team.
• Informing parents or carers.
• Temporary or permanent removal of internet or computer access.
• Referral to the Local Authority or the police, where deemed appropriate.

9.3 The designated member of the Senior Leadership Team responsible for Online safety is Gabriella Fokti, Assistant Headteacher and Deputy Designated Safeguarding Lead.

Ratified at the Teaching, Learning and Assessment committee meeting on 10th April 2024

Signed: Chair of Governors

Date: