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 including all filtering and monitoring. The school uses Policy Central to ensure that appropriate content is accessed throughout the school on any device. Where concerns are raised the assigned Senior Leader will be informed to carry out investigations. 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 (2023), the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content

- Exposure to inappropriate content, including online pornography, violence and associated offensive language through ignoring age ratings in games, images of substance abuse
- Lifestyle websites, for example pro-anorexia/ self harm/ suicide sites/ dangerous online trends
- Hate sites
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft for example ‘frape’ (hacking Facebook profiles) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being – amount of time spent online (internet or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

Commerce

- Inappropriate advertising
- Phishing
- Risk of financial scams
- Risk of online gambling

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. This policy stands alongside our Safeguarding Policy.

1.3 This policy was adopted by the governing body on *____________________ 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 expectation by Ofsted that rigorous online safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

2.2 The 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, and are users of, 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 implemented, that training in Online Safety is given high priority across the school, that consultations on the details of the arrangements for Online Safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to the governing body for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with 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 to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

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 to co-ordinate Online Safety. This person will also be a member of the Safeguarding Team answerable to the lead DSLs. 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.

Designated Safeguarding Lead

3.4 The lead for online safety will be a member of the safeguarding team. The lead DSLs should have regular updates with regards to any reported incidents relating to filtering and monitoring, and any actions taken.

- DSLs will ensure that staff are aware of how to report any concerns regarding breaches of online safety.

Network Manager

3.5 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.
- Ensuring that Users can only access the school's networks through an authorised and password protected system in which passwords are regularly changed.
- Ensuring that provision exists for misuse detection and malicious attack eg keeping virus detection up to date.
- Ensuring that the school ICT system is secure
- Ensuring that access control/ encryption exists to protect personal and sensitive information held on school-owned devices
- Ensuring that filtering and monitoring processes are rigorous through the use of Policy Central.
- Ensuring that the use of the network/ remote access/ email is regularly monitored in order that any misuse, or attempted misuse, can be reported to the designated member of the Senior Leader 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 technical information in order to effectively carry out their Online Safety role and to inform and update others as needed.
- Keeping up to date documentation of the school's online security and technical procedures.
- Ensuring that all data held on students on the school office machines have appropriate access controls in place.

Teachers

3.6 Teachers are responsible for

- Embedding Online Safety issues in all aspects of the curriculum and other school activities, where appropriate.
- Supervising and guiding students carefully when engaged in learning activities involving online technology
- Where appropriate, ensuring that students are fully aware of research skills and legal issues relating to electronic content, such as copyright laws.

All staff

3.7 All staff are responsible for

- undertaking such responsibilities as have been delegated by the Head Teacher commensurate with their salary grade and job descriptions;
- participating in training regarding Online Safety provided by the school and in consultations about this policy and about its application, including Online Safety within the curriculum;
- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the designated member of the senior leadership team for this purpose.
- Modelling safe, responsible and professional behaviours in their own use of technology
- Ensuring that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms.

Students

3.8 Expectations on students should be as follows:

- Students are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.
- Access to the internet will be supervised and monitored within the school premises.
- Only age appropriate and educational websites and applications will be accessible to students.
- Personal devices brought into school by students will be subject to approval and monitoring by school staff.
- Social media use and online communication will be closely monitored, with a focus on teaching students appropriate interaction skills.

Other users

3.9 Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in Online Safety provided by the school and in consultations about this policy and about its application, including Online Safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the designated Senior Leader.

Parents

Parents who help in the school as volunteers are covered by 3.9 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.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the designated member of the senior leadership team.

4.2 Employees, volunteers and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems;
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;

- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

4.3 Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

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

4.5 Where appropriate, students will be encouraged to report any instances of cyberbullying, inappropriate content, or online threats to a trusted adult.

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 its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of the school's data protection policy, including the requirement for secure storage of 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 take place as part of an investigation following evidence of apparent misuse.

8. Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

8.2 Any suspicions of other illegal activity should be reported to the head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

8.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

9. Handling complaints:

9.1 The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school, service provider nor the Local

Authority can accept liability for material accessed or any consequences of Internet access.

9.2 Staff and students are given information about infringements in use and possible sanctions. Sanctions include:

- interview by Head Teacher, Assistant Head Teacher (lead for Online Safety) or designated member of the senior leadership team.
- informing parents or carers
- removal of internet or computer access for a period of time
- referral to the LA or the police where deemed necessary

9.3 Our designated member of the Senior Leadership Team

Ratified at the Teaching, Learning and Assessment committee meeting on 13th March 2025

Signed:

Chair of Governors

Date: 13th March 2025