THE HALL SCHOOL

Online Safety Policy

AUTHOR: Willem Steyn and Lisa Blair

Policy ratified by: SLT

Date of publication: 1st September 2026

Date of next review: 1st September 2027

This policy is available on the school website and can be made available in large print or other accessible format if required.

Contents

1.	Scope of the Policy	4
2.	Aims and Objectives	5
3.	Roles and Responsibilities	5
3.1	Governors	6
3.2	Headmaster and Senior Leadership Team	6
3.3	Designated Safeguarding Leads	7
3.4	The ICT Manager	8
3.5	Teaching and Support Staff	8
3.6	Pupils	9
3.7	Parents	9
4.	Policy Statements	9
4.1	Access to Applications	9
4.2	Confidentiality and Data Management	10
4.3	Teaching Pupils to be Responsible Online	10
4.4	Pupil Online Safety Rules	11
4.5	Cyber Bullying	11
4.6	Staff Training	12
4.7	Parental Support	13
4.8	Governor Training	13
4.9	Technical – Infrastructure, devices	13
4.10	Data Protection and Cyber Security	16
4.11	Communications	16
4.12	Communications, Marketing, and the School Website	18
4.13	Unsuitable and Inappropriate Images	18
5.	Filtering and Monitoring	19
5.1	Filtering	19
5.2	Filtering and Monitoring Lead	20
5.3	Annual Filtering and Monitoring Review	21
5.4	Filtering and Monitoring Records	21
6.	Safe Use of Generative Artificial Intelligence	22
6.1	Generative Artificial Intelligence (AI)	22
7.	Violence Against Women and Girls (VAWG) / Misogyny	23
8.	Pupil Voice	23
9.	Handling Concerns and Responding to Incidents about Online Behaviour and Usage	25
9.1	Access to Inappropriate Websites	25
9.2	Reports of Misuse of IT Equipment and Services	26
9.3	Reports of Other ICT-related Illegal Activity	28
9.4	Safeguarding Incidents	28
9.5	Other Incidents	28
9.6	Staff Conduct	29
9.7	Sanctions	30
10.	Complaints	30
11.	Appendices	30

1. Scope of the Policy

It is the duty of The Hall to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse, and radicalisation.

New technologies are continually enhancing communication, sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Music / video downloads
- Gaming sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Applications
- Online communities via games consoles
- Virtual and augmented reality technology
- Mobile internet devices such as smart phones and tablets.
- Generative Artificial Intelligence (AI)

This policy, supported by the Acceptable Use Policies (AUPs) and the roles and responsibilities documents (for all staff, visitors, and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies and procedures:

- Acceptable Use / IT Policies;
- Staff Code of Conduct;

- Anti-Bullying Policy;
- Bring Your Own Device Procedure;
- Safeguarding and Child Protection Policy;
- Health and Safety Policy;
- Mobile Phone Policy.

2. Aims and Objectives

This policy aims to provide guidance on developing an effective online safety strategy to support staff to recognise the risks of the internet and take action. Computing is a key part of the school curriculum and one of the key aims is to ensure that pupils are aware of online safety messages. This is part of the Hall school's responsibility to safeguard and promote the welfare of pupils, as well as providing a safe learning environment. It is recognised that abuse can occur exclusively online, or technology may be used to facilitate offline abuse.

The Hall has an online safety strategy in place which is based on a framework of policy, practice, education, and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks.

From reading this policy, staff and governors should know how the School encourages the safe use of artificial intelligence and helps pupils and staff understand the risks involved:

- promotes the use of technology within the curriculum;
- protects pupils from harm;
- ensures the school fulfils its duty of care to pupils;
- provides clear expectations for staff and pupils on acceptable use of the internet; and
- safeguards staff in their contact with pupils and their own use of the internet.

The school will ensure that:

- There is a safe internet platform at the school which provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems;
- There is a culture of safe practice, ensuring that everyone is aware of expected standards of online behaviour; and
- Pupils are taught how to keep both themselves and others safe online and use technology responsibly; this should be achieved by working in partnership with parents and carers to raise awareness of potential risks of internet use.

3. Roles and Responsibilities

The key individuals regarding this policy are:

- The Safeguarding Governor

- The Designated Safeguarding Lead
- The Designated Safeguarding Team
- The ICT Manager
- The Head of Computing

It is the responsibility of the whole school as a community to uphold the school's online safety policy. This policy has the backing of the governors, is overseen by the DSL (as delegated by the Headmaster and assisted by the ICT Manager). The policy will be fully implemented by all staff members.

3.1 Governors

3.1.1 Governors have a statutory responsibility for pupil safety and should be aware of online safety issues, providing support to the Headmaster and DSL. The governing body will review this policy at least annually. Governors retain strategic responsibility for ensuring that filtering and monitoring arrangements remain effective and proportionate and will challenge and support school leaders accordingly.

Additionally, the Governors should:

- consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the ICT system along with the proportionality of costs versus safeguarding risks;
- Ensure that there are policies and procedures in place to keep pupils safe online. The Governor with Safeguarding responsibility is responsible for approving and reviewing this policy;
- Ensure their school or college has appropriate filtering and monitoring systems in place;
- Receive an annual report regarding the effectiveness of filtering and monitoring arrangements, significant online safety incidents, emerging online risks and actions taken during the year. Governors will use this information to fulfil their safeguarding oversight responsibilities.
- Do all that they reasonably can to limit children's exposure to the risks from the school's or college's ICT system as highlighted in this policy;
- Ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified;
- Be subject to the same online safety rules as all staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct; and
- Always use school email addresses when conducting School business matters.
-

3.2 Headmaster and Senior Leadership Team

The Headmaster and Senior Leadership Team have the day-to-day responsibility and a duty of care for ensuring the safety (including online safety) of members of the school community. The responsibility for online safety will be delegated to the DSL and the ICT Manager, who will work with the Digital Strategy Group to implement and ensure:

- The overall development of this policy and ensure the security and management of online data;
- The School has appropriate filtering and monitoring systems in place and regularly review their effectiveness;
- Online safety issues are given a high profile within the School community;
- There is co-operation between board of Governors and parents to promote online safety and forward the School's online safety strategy;
- Online safety is embedded in staff induction and training programmes;
- Decisions on sanctions against staff and pupils, who are in breach of acceptable use policies, are consistent; and
- Proper response to serious incidents involving online safety are taken.

The Headmaster and the DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. Should serious online safety incidents take place, either the Headmaster or the Safeguarding Governor (if the incident involves any one of the above) will be informed. They will determine what action to take. If the issue involves safeguarding concerns, then the Safeguarding and Child Protection Policy will be followed to determine whether to inform external persons/agencies.

The Headmaster, ICT Manager and DSL have a monthly filtering and monitoring meeting to discuss report on online safety.

3.3 Designated Safeguarding Leads

The DSL and deputy DSLs should be referred to for support with any online safety incident that has serious implications for the child's safety or well-being. They will decide whether a referral should be made to Children's Safeguarding and Social Work or the Police.

Through the delegation of duties, the DSL will be responsible for all responsibilities of the Headmaster as listed above. Including and in addition to the delegated duties, the DSL will:

- Arrange for the provision of training and advice for staff, parents and Governors;
- Be responsible for online safety education for pupils;
- Receive reports of online safety incidents and monitor incidents to inform future online safety developments;

- Review filtering and monitoring concerns, and respond to any safeguarding concerns. The effectiveness of the school's filtering and monitoring systems will be reviewed periodically by the DSL, other appropriate staff and governors.

- Meet as necessary with the Governor to discuss current issues;

The DSL is trained in online safety issues and made aware of the potential for serious child protection and safeguarding issues that arise from:

- sharing of personal data;

- access to illegal/inappropriate materials;

- inappropriate online contact with adults/strangers;

- potential or actual incidents of grooming;

- cyber-bullying; and

- Prevent.

3.4 The ICT Manager

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DSL. The School's ICT Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack;

- The school meets all online safety technical requirements as set out in statutory guidance;

- Users may only access the school's networks and devices if properly authenticated and authorised;

- The school has appropriate filtering and monitoring systems in place, which are regularly reviewed to evaluate their effectiveness;

- The filtering policy is applied and updated on a regular basis;

- They keep up to date with online safety technical information in order to carry out their online safety role effectively and to inform and update others as relevant;

- The use of the school's networks and devices is regularly monitored to ensure compliance with the Acceptable Use Policies (AUPs) in order that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

- The required support is given to subsequent investigations into breaches and the preservation of any evidence.

3.5 Teaching and Support Staff

All school staff have a dual responsibility regarding their own internet use, whilst also providing guidance, support, and supervision for pupils. They should:

- Adhere to this policy and other relevant procedures, ensuring that they have an up-to-date awareness of online safety matters;
- Ensure that they have read, understood, and agreed to the Staff AUP agreement;
- Recognise when pupils are at risk from their internet use or have had negative experiences and take appropriate action;
- Report any suspected incident or concern to the appropriate person for investigation;
- Ensure all digital communications with other staff, pupils and parents are on a professional level using associated School platforms and devices;
- Help pupils understand and follow this policy; and
- Help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.6 Pupils

Pupils lie at the foundation of the school, and therefore it is critical that they feel empowered to protect themselves and their cohort whilst navigating online spaces. Students are responsible for ensuring that they:

- Use the school digital technology systems in accordance with the Pupil AUP Agreements;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies, both in and out of school; and
- Understand that this policy covers their actions in both scenarios.

3.7 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents are asked to support the school in promoting good online safety practices and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events;
- Access to the Parent Portal; and/or
- Their children's personal devices in the school.

4. Policy Statements

The school has put the following measures in place to ensure the safety of all pupils whilst online at school:

4.1 Access to Applications

Social networking sites such as Facebook, Instagram and Twitter are not permitted within the school.

4.2 Confidentiality and Data Management

The school ensures that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data is held securely, and password protected, with access given only to staff members on a "need to know" basis. Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system. Any breaches of data security should be reported immediately to the ICT Manager, Headmaster and the Director of Finance (DPO).

4.3 Teaching Pupils to be Responsible Online

The Online Safety curriculum should be reinforced by all members of staff. It should be broad, relevant, and provide progression, and will be provided in the following ways:

- An Online Safety curriculum is provided as part of ICT, PSHE and other lessons and is regularly reviewed;
- Key online safety messages are reinforced as part of a planned programme of assemblies;
- Pupils are taught to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of information;
- Pupils are helped to understand the need for the Pupils (AUP) Agreement and encouraged to adopt safe and responsible use both within and outside the school;
- Pupils are helped to understand the benefits and risks associated with social media, online posting, and messaging; and
- Pupils will be taught to recognise misinformation, disinformation, manipulated media and AI-generated content and to critically evaluate online information sources; and
- Staff should act as good role models in their use of digital technologies, the internet, and mobile devices.

The school provides opportunities to teach online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered both inside and outside school will also be carried out via PSHE, as well as informally when opportunities arise. The breadth of issues classified within online safety is considerable and ever evolving, but can be generally categorised into four areas of risk, often known as the '4 Cs':

- 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 being subjected to harmful online interaction with other users or with generative AI applications that simulate human interaction.

- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving nudes and semi-nudes (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, including AI-generated material).

- commerce: risks such as online gambling, gambling in gaming, inappropriate advertising, phishing and or financial scams. If there is concern for any pupil or staff, then this concern can be reported to the Anti-Phishing Working Group (https://apwg.org/).

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy). Pupils should approach the DSL, the Deputy Designated Safeguarding Leads or the Filtering & Monitoring Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies (see 4.3 below).

4.4 Pupil Online Safety Rules

In addition to and alongside understanding and adhering to the AUP Agreement, pupils should comply with the following online safety rules:

- Access to and use of personal email accounts, unregulated public social networking sites, chat rooms and/or gaming sites on the school internet system is forbidden and is blocked;

- Pupils should be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender;

- Pupils should not disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites;

- All electronic communications should be polite;

4.4.1 Bullying or harassment via email, chat rooms and/or social networking sites will not be tolerated and will be dealt with in accordance with the school's Anti-Bullying Policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment;

- Use of the school internet system is for the purposes of education or School business only, and its use may be monitored;

- Pupils should take care when uploading personal photos of themselves or others onto sites as there is no control where images may end up or who can see them;

- Pupils should not respond to any hurtful or distressing messages but to let their parents know so that appropriate action can be taken;

- Pupils should not arrange to meet anyone whom they have only met online; and

- Pupils should not give out any financial details online.

4.5 Cyber Bullying

Cyber bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience. Cyber bullying is extremely prevalent, as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Cyber bullying may take the form of, but is not limited to:

- rude, abusive or threatening messages via email social media or text;
- posting insulting, derogatory or defamatory statements on blogs or social networking sites;
- setting up websites that specifically target a victim;
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, making, sharing or receiving nudes and semi-nudes, including AI-generated material); and/or
- excluding or removing someone from an online group (for example on WhatsApp groups).
- The school recognises that child-on-child abuse, including online bullying, can occur both in and outside of school, and all incidents will be taken seriously, recorded, and responded to in line with safeguarding procedure

To feel empowered to deal appropriately with incidents of cyber bullying, all pupils will be taught:

- to only give out mobile phone numbers and email addresses to people they trust;
- to only allow close friends whom they trust to have access to their social networking pages;
- not to send or post inappropriate images of themselves;
- not to respond to offensive messages;
- to report the matter to their parents and a member of staff immediately; and
- to preserve any evidence of bullying (for example, by taking screenshots).

In the first instance, any incidents of online bullying that involve pupils at the school, whether they take place on school premises or outside School, should be reported to the DSL. They will record the incident and ensure that the incident is dealt with in line with the school's Anti-Bullying Policy. Incidents will be monitored by the DSL and the information used to inform the development of policies.

Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration will be given to reporting the matter to the police as in these cases as the bullying may be a criminal offence.

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions.

4.6 Staff Training

All staff working with children are responsible for demonstrating, promoting, and supporting safe behaviours in their classrooms and following school Online Safety procedures.

It is essential that all staff who are granted access to the school network receive online safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and recorded as having taken place, as follows:

- Online safety training is made available to all staff and regularly enforced (at least annually). Annual safeguarding and online safety training will include emerging technologies and risks associated with generative AI, deepfakes, nudification tools, AI-enabled bullying, impersonation and misinformation; and
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand this policy. This should include training with the DSL and ICT services.

4.7 Parental Support

Parents play an essential role in the education of their children and in monitoring and regulating their children's online behaviour. Therefore, parents need to know about the risks so that they can continue online safety education at home and regulate and supervise their children's use as appropriate to their age and understanding.

4.8 Governor Training

The relevant Governor should take part in online safety training/awareness sessions. The ICT Manager and Director of Operations will advise HR what training the relevant Governor needs to do and when by. HR will give details of this training so it can be communicated to the Governor. This training must be logged by HR.

4.9 Technical – Infrastructure, devices

4.9.1 Bring Your Own Device (BYOD) and Pupil Mobile Phones

In Year 7 and 8, pupils are permitted to bring their own device to the school. The ability to do so is only permitted if the pupil understands, agrees, and/or adheres to the following:

- Users who connect their own devices to the school's network are bound by the school's policies;

- All users are provided with and accept by signature the relevant AUP agreement (Appendix 1);

- All school network systems are secure, and the wireless network is configured to require a user name and password. Users can be identified and different policies by category can be applied, as on the cabled network;

- Devices connected to the school's network are covered by the school's normal filtering systems;

- Users accessing the school's wireless networks are authenticated by their login details as above. Connection of a user's device to the school's network is recorded. Pupils will receive guidance on the appropriate use of personal devices;

- The school adheres to the principles and complies with the requirements of the Data Protection Act; and

- Pupils will receive and must follow any separate guidance on the appropriate use of personal devices.

Pupils in Year 7 and 8 are permitted to bring a mobile phone to school if they have a valid reason to do so. Parents must complete a form indicating that they give permission for their son to bring a phone to school. On the form, parents must indicate the reason why their son requires a phone at school.

On arrival at school phones must be handed in to matron and then they can be collected at the end of the school day. Pupils are very aware that they must not have a phone in their bag or on their person during the school day. This approach is monitored and the sanctions applied if a pupil does not observe this policy.

4.9.2 Staff Mobile Phones

Staff are advised to refer to the Staff Conduct of Conduct, section 13.

Staff may have mobile phones in school. The ability to do so is only permitted if the relevant member of staff understands, agrees, and/or adheres to the following:

- Staff must not use personal mobile phones to communicate with pupils;

Staff are not to use mobile phones in the classroom, during lessons. Phones are to be on 'silent' or switched off during class time.

- Phones must be kept out of sight (e.g., drawer, bag, pocket) when staff are with pupils;

- Phones should also not be used whilst on playground duty or during the teaching of a lesson outside;

- Calls/ messaging must be made/ received in private during non-contact time. As a courtesy to colleagues, calls should not be made on a mobile phone in the any of the staff rooms;

There is no obligation for a member of staff to have their school email on their phone or the iSams app;

The school has several phones / devices and cameras that can be used to communicate with parents and to record events;

- For their own protection, staff must avoid using personal mobile phones to communicate with parents via messaging services and calling. If the use of a personal mobile phone is unavoidable then the call should be logged with the relevant Head of Section – Junior, Middle and Senior.

- We expect staff to act in a responsible professional manner with regards to the use of mobile phones in school, including to facilitate communication on school business;

- It is important that a school mobile phone is available and used when a visit, event or sporting fixture is taking place away from school. A school mobile must be used on these trips, and not a personal mobile under any circumstances; and

- Mobile phones must not be used whilst driving minibuses.

Staff must immediately report to the DSL Team and/or the Filtering and Monitoring Lead the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;

- bring the school into disrepute;

- breach confidentiality;

- breach copyright;

- breach data protection legislation; or

- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;

    - using social media to bully another individual; or

    - posting links or material which is discriminatory or offensive.

4.9.3 Taking and Use of Digital and Video Images

Staff are allowed to take digital and video images to support educational aims when using a school device. They must refer to the guidance published in relation to the use of own devices and storage of media.

Staff must not take any images of pupils on a personal mobile phone or device. A school phone/device/camera must be used if an event is to be photographed.

4.9.4 Staff

Staff should always think carefully about the images they take and where these are stored.

All images once downloaded must be stored in the secured and shared area.

4.9.5 Parents

Parents, guardians, or close family members are welcome to take photographs of their own children taking part in school events, they must not take photographs of other

pupils, except incidentally as part of a group shot. Parents are reminded that such images are for personal use only, and images which identify other pupils should not be made accessible to others via the internet or published in any other way.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Parents are requested to give their permission for the use of Pupils' photographs on the School's Intranet, Website, or social media as part of their Registration for the School. Where permission is not granted, the school office will inform all staff.

Pupils must not take, use, share, publish or distribute images of others without their agreement. This is taught from Year 2 – Year 4 in the Online Safety unit (part of ICT lessons).

4.10 Data Protection and Cyber Security

The school has a Data Protection Policy which includes electronic data, which has been revised to comply with the General Data Protection Regulations (GDPR) and Data Protection Act (DPA, 2018).

The school must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove special category personal data from School premises, whether in paper or electronic form, and wherever stored, without prior consent of the Headmaster. Where a member of staff is permitted to download data off site it will need to be password protected.

There are two exceptions where prior approval is not required:

4.10.1 iSAMS, the school's data management system, may be used on personal devices provided that the device used is secure and password protected.

- For pupils on residential trips, medical information, and other relevant information (e.g., passport details) may be taken off site by the trip leader.

Staff should remain vigilant to key cyber security risks including phishing emails, weak or reused passwords, unauthorised access to systems, and the accidental sharing of sensitive data. They must ensure devices are secured with up-to-date software, use strong password practices (including multi-factor authentication where available), and report any suspicious activity or potential data breaches immediately. Staff should also be cautious when accessing school systems on personal or public networks and follow the school's data protection and acceptable use policies at all time.

4.11 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following describes how the school considers the benefit of using these technologies for education outweighs their risks/disadvantages.

These communications technologies are allowed for all pupils:

- Use of laptops in lessons, library periods and club activities with permission of a member of staff;

- Use of personal email addresses in school or on the school network;

- Mobile phones may be brought to school by Year 7 pupils and above, but they must be registered and handed to the School Matron at the start of the school day.

The school email service may be regarded as safe and secure. Users should be aware that emails leaving or entering the school are scanned for viruses, spam, and bad language.

In accordance with the AUP Agreement, users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any school-related digital communication between staff, pupils, or parents must be appropriate with the following guidelines in place:

- Staff must not give their personal email account to pupils or parents - current or former;

- Staff must not have any contact details on their personal phone for current pupils and while former pupils are in secondary education. Neither should they have contact details for current parents.

- If a member of staff receives a message on their phone from a parent, they must reply via school email;

- Staff must not put themselves in a position where they could be accused of improper behaviour by engaging in private online communications with current or former pupils and/or their parents. Such private online communications include but are not limited to messaging or being part of WhatsApp groups or other social media sites; and

- Staff must not accept current pupils as `friends' on any social networking site and must avoid accepting past pupils as `friends' until they have completed secondary education.

- Staff must immediately report to the DSL and ICT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the DSL and ICT Manager.

Any communication with current or former pupils, if required, must be made through the school email system. If an email is received from a former pupil, then any reply must also be copied to a Head of Section.

Pupils are provided with individual school email addresses for educational and administrative use for the period of their studies at the school, which remain active for a further 3 months. Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are reminded of the need to communicate appropriately when using digital technologies.

On the school website, only school email addresses should be published. Staff should use school email for school business.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring The Hall School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

4.12 Communications, Marketing, and the School Website

Content will not be uploaded onto the school's external facing website unless it has been authorised by the Head of Communications and Marketing, and in consultation with SLT, who is responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law. Links to any external websites will be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email, and telephone number. No contact details for pupils will be contained on the website. Children's full names are not published on the website or on social media.

Where photographs or videos of pupils are used for promotional purposes or advertising on the website, written permission will be obtained first from their parents or carers, who will be informed of the purpose of the image and where it will appear.

Pupils' full names should never be published where their photograph or video is being used or published. The school will inform parents that, as stated above, although they may take photographic images of school events that include other pupils, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

4.13 Unsuitable and Inappropriate Images

The school believes that the activities referred to in the following section would be inappropriate and that users, including all staff and students, should not engage in these activities in school or outside school. Whilst this list is not exhaustive, the school policy restricts usage as follows.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals, or comments that contain or relate to:

- Child sexual abuse images — The making, production, or distribution of indecent images of children contrary to The Protection of Children Act 1978;

- Grooming, incitement, arrangement, or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003;

- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008;

- Criminally racist material in UK — to stir up religious hatred (or hatred on the grounds of sexual orientation) — contrary to the Public Order Act 1986;

- Statements or images that are intended to radicalize individuals or groups or in any other way endorse, condone, or incite extremist or terrorist activity;

- Using school systems to access pornography & adult material;

4.13.1 Deepfakes and AI-generated imagery, including manipulated images, audio or video designed to humiliate, exploit, harass, impersonate or otherwise cause harm to another person, including sexualized deepfakes involving pupils or staff;

- Promotion of any kind of discrimination;

- Threatening behaviour, including promotion of physical violence or mental harm;

- Any other information which breaches the integrity of the ethos of the school or brings the school into disrepute;

- Using school systems to run a private business;

- Using systems, applications, websites or other mechanisms that deliberately bypass the filtering or other safeguards employed by the school;

- Revealing or publicising confidential or proprietary information (e.g. financial/ personal information, databases, computer/network access codes and passwords);

- Creating or propagating computer viruses or other harmful files;

- Online gaming for education and/or non-educational purposes;

- Online gambling;

- File sharing (peer-to-peer);

- Using school systems to access social media;

- Using school systems to create and/or upload video broadcasts; and/or

- Using school systems to access and use of messaging apps.

5. Filtering and Monitoring

5.1 Filtering

The school's IT systems have filters and monitoring systems in place such as Securly, which sort hundreds of thousands of websites, differentiating types of sites such as adult gaming versus educational gaming, promoting a safe digital learning experience.

- **Protecting** – the school uses Sophos software to provide protection against outside cyber attackers by shielding school computers and networks from malicious and unnecessary network traffic.

- **Supervision** – pupils will receive age-appropriate supervision when using the internet. Pupils should not be allowed to aimlessly "surf" the internet. The location of internet enabled devices in classrooms and teaching areas are placed to allow an appropriate level of supervision;

- **Planning lessons** – staff should plan the use of internet resources ahead of lessons by checking sites and storing information offline where possible. Where staff require access to blocked websites for educational purposes, this should be discussed and agreed with IT support to remove those sites. Any request to do so should be audited by the IT Manager, and clear reasons for the need must be established and recorded.

- **Information Security** – the level of security protection procedures are reviewed periodically to keep up with evolving cyber-crime technologies.

- **Access Management** – access to the school's internet system is via individual logins and passwords for staff and pupils. Staff are required to use multi-factor authentication. The IT Department keep a record of all logins used within the school for the purposes of monitoring and auditing internet activity. Network and technical staff responsible for monitoring systems are supervised by a senior member of their management team.

It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. As part of this process the school has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness. The school fully complies with the Department for Education's published filtering and monitoring standards which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.

- review filtering and monitoring provision at least annually.

- block harmful and inappropriate content without unreasonably impacting teaching and learning.

- have effective monitoring strategies in place that meet their safeguarding needs.

Roles and responsibilities for filtering and monitoring at the School:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as laid out in the Internet Security Information document (Appendix 3).

- The ICT Manager continually reviews and audits the safety and security of school technical systems (supplemented by an external audit and review annually).

- Servers, wireless systems, and cabling must be securely located and physical access restricted.

- All users are provided with a username by ICT Support. They must then create their own secure password. Users are responsible for the security of their username and password.

- Internet access is filtered for all users. The firewalls check for an updated filter list daily. If a URL is not on the filter list, the firewall checks the manufacturer's database directly. This database is updated constantly.

- A system is in place for users to report any actual or potential technical incident or security breach.

- Security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date anti-virus and anti-malware software.

5.2 Filtering and Monitoring Lead

The School has appointed a member of the Senior Leadership Team as the designated Filtering and Monitoring Lead/Champion; Lisa Blair (DSL and member of SLT). The Filtering and Monitoring Lead is responsible for ensuring that the School's filtering and monitoring arrangements are effective, proportionate, and aligned with safeguarding requirements. The role is undertaken in partnership with the Designated Safeguarding Lead (DSL) and ICT Manager. KCSIE 2026 requires schools to identify an SLT lead responsible for filtering and monitoring and to ensure formal review arrangements are in place.

The Filtering and Monitoring Lead will:

- Oversee the effectiveness of filtering and monitoring systems.

- Ensure online safety risks are appropriately considered within the school's safeguarding arrangements.

- Work with the Headmaster, DSL and ICT Manager to review incidents, trends and emerging risks.

- Ensure that filtering and monitoring reviews are completed and documented.

- Report relevant findings and recommendations to the Headmaster and Governors.

- Ensure that the school's filtering and monitoring arrangements continue to meet the needs of pupils, staff and the wider school community.

5.3 Annual Filtering and Monitoring Review

- The effectiveness of the School's filtering and monitoring arrangements will be formally reviewed at least once every academic year. The review will be led by the Filtering and Monitoring Lead (Lisa Blair, DSL), with support from the Headmaster and ICT Manager. Findings will be documented and reported to Governors.

- The annual review will be formally recorded and retained for inspection and governance purposes.

The review will consider:

- Whether filtering systems appropriately block harmful and inappropriate content.
- Whether monitoring systems effectively identify safeguarding concerns.
- The suitability of arrangements for different age groups.
- The effectiveness of filtering and monitoring across all school-owned and authorised personal devices.
- Emerging safeguarding risks, including those associated with generative artificial intelligence.
- Any incidents, trends or concerns identified during the previous academic year.
- Actions resulting from the review will be recorded and tracked to completion.

Emerging Technologies and Artificial Intelligence

As part of the annual review of filtering and monitoring arrangements, the School will consider the safeguarding implications of emerging technologies, including generative artificial intelligence (AI) tools. This will include assessing whether existing filtering, monitoring, reporting procedures, staff training and pupil education remain effective in identifying and mitigating online safety risks associated with AI-generated content, deepfakes, nudification applications, misinformation and other evolving technologies.

-

5.4 Filtering and Monitoring Records

The School will maintain records demonstrating the operation and effectiveness of filtering and monitoring arrangements. These records may include:

- Annual review reports.
- Records of testing undertaken.
- Logs of filtering incidents.
- Monitoring alerts and actions taken.
- Changes made to filtering settings.
- Reports made to the DSL.
- Governor oversight and review records.
- These records provide evidence that the School is meeting its safeguarding responsibilities
- And support continuous improvement of online safety arrangements.

6. Safe Use of Generative Artificial Intelligence

6.1 Generative Artificial Intelligence (AI)

The School recognises that generative AI tools can support learning, creativity and administrative efficiency. However, AI systems can also present safeguarding, privacy, accuracy and ethical risks. The School recognises that artificial intelligence technologies continue to evolve rapidly. As part of its wider safeguarding and online safety arrangements, the School will periodically review emerging AI technologies and assess associated safeguarding risks, ensuring that policies, procedures, filtering and monitoring arrangements, staff training and pupil education remain appropriate and effective. Staff and pupils must therefore use AI technologies responsibly and in accordance with this policy, the Acceptable Use Agreements, the Data Protection Policy and

Safeguarding Policy. KCSIE 2026 specifically identifies AI-generated content and deepfakes as online safety risks which schools should address.

6.1.1 Staff

When using AI tools, staff must:

- Only use approved or authorised AI services for school purposes.
- Exercise professional judgement and not rely solely on AI-generated outputs.
- Verify the accuracy of AI-generated information before using or sharing it.
- Not upload confidential, personal, safeguarding or special category data into AI systems unless formally approved and compliant with data protection requirements.
- Report any safeguarding concerns arising from AI-generated content immediately to the DSL.

6.1.2 Pupils

Pupils may only use AI tools under staff direction or in accordance with specific school guidance. Pupils will be taught to:

- Critically evaluate AI-generated information.
- Understand that AI systems can produce inaccurate or misleading content.
- Use AI responsibly and ethically.
- Report harmful or concerning AI-generated content.
- Understand the risks associated with sharing personal information with AI systems.

6.1.3 AI Misuse

The School will treat the following as serious concerns:

- Creation or sharing of AI-generated intimate images.
- Deepfakes and AI-generated imagery, including manipulated images, audio or video intended to humiliate, harass, bully, exploit or impersonate another person, including sexualised deepfakes of pupils or staff.
- AI-enabled bullying, harassment or impersonation.
- Use of AI to facilitate grooming, abuse or deception.
- Uploading personal or confidential information into unauthorised systems.

The School recognises the risks presented by AI-generated imagery, including deepfakes and so-called "nudification" applications that create real or simulated intimate images without consent. Any use of such technology involving pupils or staff will be treated as a safeguarding concern and managed in accordance with safeguarding procedures.

The School may use approved AI tools for legitimate educational, administrative, marketing, accessibility or safeguarding purposes where such use complies with data protection, copyright and safeguarding requirements.

7. Violence Against Women and Girls (VAWG) / Misogyny

7.1.1 Online Sexual Harassment, Misogyny and Violence Against Women and Girls

The School recognises that online abuse can include sexual harassment, sexualised language, misogyny, coercive behaviour, the sharing of harmful content and attitudes which normalise violence against women and girls.

Such behaviours may occur online, offline, or through a combination of both.

The School adopts a zero-tolerance approach to:

- Sexual harassment.
- Misogynistic language or behaviour.
- Sexist comments or online content.
- Sharing sexualised or degrading material.
- The creation or distribution of sexualised deepfakes.
- Gender-based bullying and discrimination.

Incidents will be recorded, investigated and managed through safeguarding and behaviour procedures as appropriate. Pupils will be educated about respectful relationships, consent, empathy and responsible online behaviour through the curriculum and wider pastoral programme.

8. Pupil Voice

8.1 Policy Statement

The Hall places a strong emphasis on **pupil voice as a central component of its safeguarding culture**. The school ensures that pupils are encouraged, enabled, and supported to express concerns, share views, and seek help. Systems are in place across all three sites to ensure that pupils know how to raise concerns and are confident that they will be listened to and responded to appropriately.

8.2 Promoting Pupil Voice

The school actively promotes a culture in which pupils feel safe to speak openly. Staff consistently reinforce the message that pupils' views are valued and that raising concerns is both expected and encouraged. Pupils are taught, in an age-appropriate manner, how to recognise worries and how to seek support.

8.3 Safe Adults

Pupils are supported to identify **safe adults** within the school community.

8.4 The role of safe adults, including the **Designated Safeguarding Lead (DSL)** and **Deputy Designated Safeguarding Leads (DDSLs)**, is clearly communicated to pupils.

- Safeguarding posters are displayed across **all three school sites**, providing clear visual reminders of who pupils can speak to if they have concerns.

8.5 Pupils are regularly reminded that they may approach any safe member of staff, with safeguarding leads always available for support.

8.6 Reporting Systems

The Hall has established **robust, age-appropriate reporting mechanisms** to ensure concerns can be raised easily and discreetly:

8.7 **'Tell Me' boxes** are available in the Junior School, 'worry' boxes in the Middle School & online concern forms in the Senior School to enable pupils to report worries/concerns privately.

8.8 In the **Junior School**, the **Zones of Regulation** framework is embedded, supporting pupils in identifying emotions and communicating concerns effectively. These continue in the Middle School in PSHE lessons & developed further through the PSHE schemes of work.

- Reporting systems are monitored by staff, and all disclosures or concerns are acted upon promptly in line with safeguarding procedures.

8.9 Curriculum and Structured Opportunities

The curriculum provides regular and planned opportunities for pupils to express opinions and safeguarding concerns:

- **PSHE lessons** explicitly address wellbeing, relationships, emotional literacy, personal safety, and help-seeking behaviours.
- **ICT lessons** include online safety education, enabling pupils to recognise risk and understand how and when to report concerns.
- Teaching is progressive, age-appropriate, and reinforces safeguarding messages consistently.

8.10 Safeguarding Education and Awareness

Safeguarding awareness is reinforced through a range of whole-school initiatives:

- **Safeguarding assemblies** are delivered across all three sites, reinforcing key messages regarding pupil safety, trusted adults, and speaking up.
- The school takes part annually in **Safer Internet Day**, strengthening pupils' understanding of online risks and reporting pathways.
- The school hosts **NSPCC workshops** for **Year 2 and Years 5 and 6**, providing specialist, age-appropriate education on personal safety, boundaries, and trusted adults.

8.11 Listening and Responding to Pupils

All pupil concerns are treated seriously. Staff are trained to:

- respond calmly and sensitively
- reassure pupils appropriately
- follow safeguarding procedures without delay

Pupils are reassured that concerns will be handled with care and confidentiality, in accordance with statutory guidance and the school's safeguarding policy.

8.12 Monitoring and Review

The effectiveness of pupil voice systems is reviewed regularly as part of the school's safeguarding oversight. Feedback from pupils, staff training, and safeguarding audits are used to ensure that procedures remain effective, accessible, and consistently applied across the school.

9. Handling Concerns and Responding to Incidents about Online Behaviour and Usage

The school aims to follow the steps set out below should a member of staff have a concern about a pupil's online usage:

- **Identify** – Pupils and parents are encouraged to pass on any concern regarding online behaviour and/or safety to a trusted member of staff. Staff are trained to handle disclosure or concerns passed to them and know how to respond and who to escalate the issue to. Staff are also trained to spot online concerns.

- **Intervene** – When staff spot a concern they will intervene or pass it onto the DSL. Safeguarding members of staff have enhanced training around handling such concerns.

9.1 **Escalate** – Concerns will always be taken seriously and escalated appropriately. Incidents of cyber bullying will be handled in line with the school's Anti-Bulling and Behaviour Policies. Cases involving nude or semi-nude images will be handed in line with the school's Safeguarding and Child Protection Policy. Any online child-on-child abuse will be handled in line with the school's Safeguarding and Child Protection Policy.

- **Report** - all incidents and complaints relating to online safety and unacceptable internet use will be reported to the DSL, who will decide as to whether to refer the matter to the police and/or Children's Safeguarding and Social Work. Where the incident or complaint relates to a member of staff, the matter must always be referred to the DSL for action under staff conduct policies for low level incidents or consideration given to contacting the LADO under the relevant DfE and Local Authority guidance on dealing with allegations against staff where this is appropriate. The DSL will keep the Headmaster informed of such incidents. Incidents involving the Headmaster should be reported to the chair of the board of Governors;

- **Record** – all incidents, involving pupils, must be recorded by the relevant member of pastoral staff as an online safety issue to allow monitoring;

- **Monitor** – The School's DSL will review the log of all online safety incidents and complaints, as well as reviewing the Low-Level Concerns Log regularly for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system and use these to inform and update this policy.

9.2 Access to Inappropriate Websites

Unintentional Access by Pupils and/or Staff:

- If a pupil or staff member accidently opens a website that has content which is distressing or upsetting or inappropriate, staff should immediately (and calmly) close or minimise the screen or request that the pupil does so.

- Staff should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.

- The incident should be reported to the DSL and details of the website address and URL provided.

- The DSL should then liaise with the ICT Manager or learning platform provider to ensure that access to the site is blocked, and the school's filtering system reviewed to ensure it remains appropriate.

Intentional access by a pupil:

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the AUP Agreement and Behaviour Policy and be subject to appropriate sanctions.

- The incident should be reported by the staff member to the DSL and details of the website address and URL recorded.

- The DSL should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.

- The relevant member of pastoral staff will be asked to speak to the pupil's parents about the incident and what action will be taken and logged.

Intentional access by a member of staff:

- All concerns about staff should be reported to the Headmaster (or their named deputy as outlined by the school's whistleblowing policy). If the misconduct involves the Headmaster or a Governor, the matter should be reported to the Chair of the Board of Governors.

- The DSL will notify the network manager so that the computer, laptop, or other device is taken out of use and securely stored to preserve any evidence. A note of any action taken should be recorded.

- The DSL will arrange with the network manager or learning platform provider to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the DSL will liaise with the Headmaster and HR, and they will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.

- If the materials viewed are illegal in nature the DSL, in liaison with the Head, should report the incident to the police and follow their advice.

9.3 Reports of Misuse of IT Equipment and Services

Misuse may originate from these sources and by these means:

9.3.1 IT Support:

- From daily filter log reports.

- Through routine examination of firewall and other service logs.

- By alerts raised from desktop monitoring software.

- From materials discovered during routine or other maintenance of school-owned ICT equipment – including servers, desktop and laptop computers, and mobile devices.

- As a result of observations of unusual patterns of network and storage use.

9.3.2 Complaints concerning ICT activity made to the school from:

- Pupils
- Parents
- Staff
- Others outside the community

9.3.3 Staff:

- Suspicions of ICT misuse by staff and/or pupils.
- Staff members or pupils who wish to confess to some wrongdoing.

9.3.4 Anyone suspecting that:

- accesses have been attempted to any website containing child abuse images;
- accesses have been attempted to any website containing material that breaches the Obscene Publications Act;
- accesses have been attempted to any website containing criminally racist material;
- accesses have been attempted to any website which contains statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity;
- any such materials are themselves to be found on any electronic device - whether owned by the school or not; and/or
- there has been any incident by electronic means of 'grooming' behaviour must report all allegations, complaints, concerns or suspicions directly to the Headmaster or, in his absence, to the Chairman of Governors, unless that person is the subject of the concern; those about the Headmaster should be reported to the Chairman of Governors (or in his absence, the Vice Chairman). All allegations, complaints, concerns, or suspicions about the Chairman of Governors should be reported to the LADO without the Chairman of Governors being informed. The LADO may choose to appoint a `case manager'.

Action from this point will be dictated by the Safeguarding and Child Protection Policy and Procedures.

9.4 Reports of Other ICT-related Illegal Activity

Concerns, suspicions, or allegations of other ICT related illegal activity (such as fraud, copyright theft or unlicensed use of software) by a member of staff should also be reported according to the reporting hierarchy outlined above. Such concerns will be managed in accordance with the school's whistleblowing code.

Concerns that relate to the illegal behaviour or actions of pupils or parents (and not staff) should be reported to the DSL or in her absence, a Deputy DSL. The DSL (or Deputy) will follow the

Safeguarding and Child Protection Policy and Procedures in reporting any such behaviour to children's social care and/or the police.

Suspicions of other ICT related illegal activity (such as fraud, copyright theft or unlicensed use of software) should be reported directly to the Head.

9.5 Safeguarding Incidents

Substantive safeguarding concerns should be reported to Headmaster (if concerns relate to activity of a member of staff) or to the DSL (if about pupils) as per the Safeguarding and Child Protection Policy and Procedures.

9.6 Other Incidents

Reports of misuse of ICT equipment and services originating from:

- individuals which do not raise safeguarding concerns or appear to suggest any other kind of illegal activity, should be made directly to the ICT Manager and/or DSL as necessary to establish, capture and preserve any relevant data or other evidence.

If further investigative actions are required these may include but are not limited to:

- Detailed examination of firewall, filter, mail relay and other security logs, and the extraction there from of references to activity associated with the incident in questions;

- Examination of materials stored on the school's storage networks, taking copies of any items associated with the incident in question;

- Remote examination of the school desktop and laptop computers, and the gathering of relevant evidence therefrom, including the copying of materials or the taking of screen captures as required;

- Examination of the contents of the school's email mailboxes, including sent and deleted items, and the extraction of messages and materials relevant to the incident in question; and/or

- The requiring of staff to return School-owned mobile devices to the ICT Manager for investigation.

These investigations will be carried out by the ICT Manager. Unsuitable materials will be copied and may then, under the direction of the appropriate authority, be deleted from storage, mailboxes, and/or computers.

At the culmination of the investigation a report will be passed on to the Headmaster. The report will include all materials and references found and will detail the processes followed. The relevant names will be redacted as appropriate from all such reports in accordance with confidentiality requirements.

Should any of these investigations uncover materials which there is any suspicion of illegality, the ICT Manager (in consultation with the Headmaster) will immediately suspend any further inspection. The ICT Manager will report the matter in accordance with the procedure above (illegal incidents) or to the police (if already involved) and await direction from them. ICT staff will also assist with the recovery of School-owned equipment such as desktop and laptop computers and mobile devices as required by the relevant authorities.

The ICT Manager will only examine the contents of devices not owned by the school with the prior agreement of the pupil and/or his parents.

9.7 Staff Conduct

Staff should be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use ensuring that it complies with the school's policies, particularly in terms of contact with pupils.

The school has clear policies available to staff on expectations for online behaviour detailed in the Staff Code of Conduct and the School's Safeguarding and Child Protection Policy, as well as the Staff AUP Agreement (Appendix B).

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations:

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips. Staff should always use school equipment and only store images on the school computer system. Personal devices should never be used in this context;

- Staff should take care regarding the content of, and access to, their own social networking sites and ensure that pupils and parents cannot gain access to these;

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal;

- Staff should be particularly careful regarding any comments to do with the school that are communicated over the internet. Remarks that are private may go to a wider audience and raise questions regarding confidentiality;

- Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute;

- Staff should not engage in any conversation with pupils via instant messaging or social networking sites;

9.7.1 Where staff need to communicate with pupils regarding schoolwork, this should be via official school channels i.e. Teams. Messages should be carefully written to ensure that they are clear, unambiguous, and not open to any negative interpretation;

- When contacting parents or pupils by telephone, staff should only use school equipment;

- Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should not lend their mobile phones to pupils;

- When contacting parents or pupils by email, staff should always use their school email address or account. Personal email addresses and accounts should never be used;

- Staff should ensure that personal data relating to pupils is stored securely. Laptops should be encrypted, and iPads protected with a strong password; and/or

- Where staff are using mobile equipment provided by the school, they should ensure that the equipment is always kept safe and secure.

  When staff leave, their line manager should liaise with the network manager to ensure that any school equipment is handed over **before they depart** and that PIN numbers, passwords and other access codes are reset so that the staff member can be removed from the school's ICT system.

9.8 Sanctions

9.8.1 Pupil Sanctions

Sanctions will be applied for pupil breaches of the Pupil AUP Agreement in line with the Behaviour Policy. Sanctions relating to harmful sexual behaviour online or other aspects of pupil-on-pupil abuse will aim to promote the school's zero tolerance to such abuse.

9.8.2 Staff Sanctions

Staff sanctions for breaches of the Staff AUP Agreement will reflect the seriousness of the breach and will reflect their position of trust and the need to ensure acceptable standards of behaviour by adults working with children. Sanctions will be applied in line with the Staff Code of Conduct and any other relevant Government policies and legislation.

10. Complaints

10.1 As with all issues of safety at The Hall, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate.

10.2 Incidents of or concerns around e-safety will be recorded and reported to the school's DSL, in accordance with school policy.

11. Appendices

Appendix A - Pupil AUP agreement

Appendix B - Staff AUP agreement

Appendix C - Internet Security Information

1. Appendix A: ICT Acceptable Use Policy for Pupils

1.1 This AUP Agreement and the following regulations apply to all electronic media, including but not limited to mobile and smart technology and services that are:

- Accessed on or from the school premises.
- Accessed on School equipment and/or computers (eg. laptop, computer, iPad)
- Accessed on The School's systems or networks, and/or

1.2 Accessed through the Pupil's own personal devices on the school's premises or where it is used in a manner which identifies or associates the individual user with the school. This agreement is intended to encourage responsible and safe use of digital technologies. By acting with care and thought, pupils should be putting into practice much of this policy.

1.3 The school provides both networked, desktop computers and wireless access to the internet through its own filtered connection. Wireless access is available everywhere in the school for pupils to use if given permission to do so.

1.4 This policy must be read and countersigned by parents and/or carers and pupils.

Initials	Policy ID	Policy Statement
Personal Safety and Responsibility		
	1.1	I understand that the school will log and monitor my use of computers, devices, and my digital communications.
	1.2	I understand that if I use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment.
	1.3	I will use my @hallschool.co.uk account responsibly for all schoolwork and communications with or related to the school.
	1.4	I will keep my school username and password safe and secure. I will not share it, nor will I try to use another pupil's or staff member's username and password. I understand that I should not write down or store passwords where it is possible that someone may steal them.
	1.5	I will be polite and responsible when I communicate with others. I will not send messages either anonymously or pretending to be someone else and I will not send group messages.
	1.6	I understand that once something is posted online or written in an email, it has a permanence that is not like something that is spoken. I understand that I must take responsibility for my actions online and I should consider my reputation, the reputation of others, and the reputation of the school.
	1.7	I will not give out personal information about myself or others that could be used to identify me, my family or my friends (e.g. addresses, email addresses, phone numbers, information about the school) unless a trusted adult has given me permission to do so.
	1.8	I will not open a hyperlink in any email or attachment to an email if I have any concerns about it or think it may contain a virus or other harmful programme.
	1.9	If I see anything unpleasant or inappropriate or receive a message I do not like, I will not respond but I will save it and talk to a trusted adult as soon as possible.
	1.10	I will not view or change other people's files without their permission. I will only edit or delete my own files.

	1.11	I will not take or distribute images of anyone without their permission.
	1.12	I will never arrange to meet someone I have only ever previously met online.
	1.13	I understand that some websites and social networks have age restrictions, and I will respect this. I will not visit sites I know to be unsuitable.
	1.14	I understand that printing at The Hall School is a privilege and that I must be mindful of other users and of the environment when I do choose to print. I will not print, use colour ink, or wastepaper unnecessarily.
Device Security		
	2.1	I will only use my personal devices (laptop, kindle, iPad etc.) in school if explicit permission has been granted by a member of staff to facilitate teaching and learning. Otherwise, my laptop will stay in its jacket or in my satchel. Non-portable devices must not be moved, relocated, or adjusted without the permission of a member of staff.
	2.2	I understand that it is forbidden to use laptops during breaks in any part of the school (including form rooms) except in the following 2 cases: 1. During wet breaks: the use of laptops is only allowed for work purposes and not for playing games. 2. During cold weather breaks between October half-term and Easter: laptop use is authorised in specified areas of the school and the use of laptops is only allowed for work purposes and not for playing games.
SS only	2.3	Senior school students: I will ensure that my laptop has been fully checked by Mr. Sulek and Mr. Bukenya at the start of the academic year (and at any other time as requested) and I will bring my laptop, fully charged, to school and to each of my lessons.
MS only	2.4	Middle School students: When I have been using a school laptop from one of the carts, I will ensure that I have logged off and plugged the laptop back on charge in the correct position in the laptop cart.
	2.5	I will not install, attempt to install, or store programmes or software on any school device, nor will I try to alter the computer settings. I will not install or store programmes or software on my personal device which are contrary to the spirit of this agreement.
	2.6	I will not try to upload, download, or access any materials which are illegal, or encourage illegal, extremist or terrorist activity, or which may cause harm or upset to others, nor will I try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials (including VPN or VPN extensions).
	2.7	I will not leave any school device, or any device connected to the school network, logged on for others to use.

	2.8	I understand that I must only use the school-provided filtered Wi-Fi networks. I will not use any other unfiltered Wi-Fi connection while on school property or attending school events (it is not allowed to use Hot Spots or open unfiltered connections such as BT Wi-Fi or other subscriptions).
	2.9	I will report immediately any known issues, damages or faults involving school equipment or software, whether incidental or otherwise.
	2.10	I will report any actual or potential technical incident or security breach to a member of staff straight away.
	2.11	I understand that I must use the School's WIFI responsibly. I understand that if found to be seeking out or accessing inappropriate sites that do not meet the educational objectives of the school by using personal LTS (e.g 3G or 4G) services, I will be subject to the appropriate disciplinary sanctions, in accordance with school policy.
	2.12	I understand that any deliberate attempt to damage or 'hack' into the School's ICT infrastructure will result in disciplinary action that may include temporary or permanent exclusion from the school.
Mobile Devices		
SS only	3.1	Senior school students: If I bring my mobile phone in to school, I will hand-in my phone to matron at the beginning of the day and only retrieve it before heading home at the end of day.
MS only	3.2	I understand that I am not permitted to bring my mobile phone in to school.
	3.3	1.5 I understand that I must not share images of other students which may come under the offence of making, sharing or receiving nudes and semi-nudes. I understand that in additional to safeguarding procedures, the school will likely regard such incidents as disciplinary matters.

I agree to comply with the rules and regulations set out in The Hall ICT Acceptable Use Policy Agreement. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. If I am unable to follow the expectations set out above, the school's behaviour system will be used, however, some incidents (eg. inappropriate searches and gaming) will result in an immediate Head of Year breaktime detention and consequences shall be escalated for repeat occurrences.

Date:	Form:		Signed
		Student:	
		Parent/Carer:	

2. Appendix B. ICT Acceptable Use Policy for Staff

2.1 This agreement is intended to encourage responsible and safe use of digital technologies at The Hall. By acting with care and thought you should be putting into practice all this policy. Every member of the community must take responsibility for their actions online.

2.2 This document sets out current policy and practice and is part of the induction process for all new staff. This policy applies to all members of the school community who use School IT systems as a condition of access (whether remotely or locally), including the use of own devices for School business.

2.3 The School's ICT facilities must be used in accordance with the policy and guidelines set out in this document. This includes electronic services such as email, internet access and all other online activity. All staff and pupils should be committed to conforming to good practice in this area. Use of the School's ICT facilities implies acceptance of the conditions of use.

2.4 The Staff Acceptable Use Policy Agreement is intended to ensure that:

- Staff will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal, and recreational use when in school, when using school systems and equipment, and when connected to the school network.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

2.5 Access to ICT is made available to staff to enhance their work and to enhance opportunities for pupils' learning, and the school expects staff to be responsible users.

Initials	Policy ID	Policy Statement
Acceptable Use Policy Agreement		
	1.1	I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I understand that any property belonging to the school should be treated with respect and care.
	1.2	I understand that this policy applies when using the school's computers (e.g., laptop, computer) and systems, or my own personal device on school premises or where it involves membership of the school community.
	1.3	I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.
	1.4	I will ensure appropriate use of ICT, in any interactions with pupils.

	1.5	I confirm that I have read and understood The Hall Online Safety Policy.
	1.6	I understand all school-owned portable devices must be returned to the IT Office by dates agreed with the IT Department and Line Manager. Failure to do so will result in the cost of the device (the market value at the time of leaving) being deducted from the final salary
	1.7	I understand that the use of any of the School's ICT facilities for commercial gain (including advertising) or for work on behalf of others is prohibited unless the user has explicit prior written permission of the Senior Team
For my professional and personal safety		
	2.1	I understand the school will monitor my use of its ICT systems and networks.
	2.2	I understand that the school will log and monitor my use of computers, including my own personal devices and my digital communications whilst on school premises.
	2.3	I understand that the rules set out in this agreement also apply to use of school ICT systems out of school, and to the transfer of personal data out of school.
I understand that the security of my account is my responsibility and that I should:		
	3.1	Log on only as myself.
	3.2	Keep my login details private and make them secure.
	3.3	Not leave any device logged in and accessible to others.
	3.4	I will report any actual or potential technical incident or security breach to the ICT Manager.
I will immediately report any illegal, inappropriate, or harmful material I become aware of when in school or connected to the school network:		
	4.1	Material that appears to originate from sources external to the school should be reported to ICT Support.
	4.2	Material that appears to have been sent or circulated by a pupil or parent should be reported to the Designated Safeguarding Lead (DSL) (or in their absence a Deputy DSL)
	4.3	Material that appears to have been sent or circulated by a member of staff (including a temporary member of staff or volunteer) should be reported to the Headmaster.
I will be professional in my communications and actions when using school ICT systems at school, when using school ICT systems and equipment or when connected to the school network:		

	5.1	I will ensure that when I take and / or publish images of others I will do so in accordance with the school's policy on the use of digital / video images.
	5.2	I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
	5.3	Any use that I make of chat and social networking sites will be in accordance with the guidance given in The Hall Code of Conduct.
	5.4	I will not engage in any on-line activity that may compromise my professional responsibilities.
	5.5	I understand that the school ICT systems are primarily intended for educational use.
The school has a responsibility to provide safe and secure access to ICT:		
	6.1	I will not open any hyperlinks in emails, or any attachments to emails, unless the source is known and trusted.
	6.2	I will not try to upload, download, or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others.
	6.3	I must not use School ICT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which is either illegal (e.g., in breach of copyright law; plagiarism) and/or can reasonably be judged to be offensive, obscene, indecent, abusive or likely to incite racial hatred
	6.4	I must not use the School's ICT facilities to place, disseminate or receive materials which discriminate or encourage discrimination on, for example, the grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin.
	6.5	I will not try to use any programs or software to bypass the school's filtering and security systems in order to access such materials.
	6.6	I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Data Protection Policy.
	6.7	I understand that data protection requires that any staff or pupil data to which I have access must be kept private and confidential.
	6.8	I will immediately report any damage, loss or faults involving school equipment or software to ICT Support.
	6.9	I understand that School ICT facilities, except for portable devices, must not be moved or disconnected without the express consent of the ICT Department.

When using the internet in my professional capacity or for school-sanctioned personal use:		
	7.1	I will ensure that I have permission to use the original work of others in my own work.
	7.2	Where work is protected by copyright, I will not download or distribute copies (including music and videos).
I understand that this AUP Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises.		
I understand that if I fail to comply with this AUP Agreement, I could be subject to disciplinary action. I agree to comply with the rules and regulations set out in The Hall ICT Acceptable Use Policy Agreement for staff.		
Signed:		
Name:		

3. Internet Security Information

Risks Related to Internet Use	Details	Online Safety implication	Mitigation
Access			
Unauthorised access - by those within and outside the school	Use of School systems without permission	Yes	The school's network and systems can only be accessed by use of a network account - identified by a username and password. Network account details are only handed over in person after an induction.
Security of network accounts	Insecure passwords - sharing of accounts - revealing account details - attempting to use another's account	Yes	Strong passwords are enforced, and staff and pupil inductions reinforce the importance of network account security - and the users' responsibilities therefore. Forgotten passwords will only be reset by a member of the ICT team.
Accountability - AUPs	Non-compliance with School policies	Yes	The School's Acceptable Use Policies are signed annually
Attacks on Infrastructure			

Viral attacks	Viruses, worms, trojans		The school runs an application layer firewall. The firewall provides antivirus, threat protection and URL filtering services. All the School's servers and desktop systems run additional endpoint antivirus software
Malware	Malware, spyware, adware, ransomware		Covered by firewall and Sophos endpoint protection
Denial of service attacks	Attempts to interfere with legitimate traffic by flooding the network		Firewalls prevent all currently known DoS attacks. The configuration of the school's networks and of the security rules on the firewalls further mitigates this and other attacks
Exploitation of software vulnerabilities	Exploitation of known vulnerabilities in operating systems and applications		Threat protection cover. Regular updates and patching.
Attempts to access infrastructure equipment and services	Attempts to log on to or otherwise interfere with infrastructure equipment such as firewalls, switches, and routers		The school's network is configured such that management access to infrastructure items is only possible by ICT staff
Installation or use of unauthorised software on School systems			School systems are locked against the installation or re-configuration of software by users.

Hacking, cyber espionage from outside the school	Keyloggers, password crackers,		Threat protection service
Antisocial Use			
Bandwidth hogging	Use of applications the consume unreasonable amounts of bandwidth		Firewall is configured to prevent the use of heavy bandwidth applications such as peer to peer files sharing. Network bandwidth use is constantly monitored to identify abuses.
Running unauthorised services	Connection of a device to the school network that advertises unauthorised websites or other services		The firewall is configured in such a way that only authorised sites and services can be publicised from the school's network to the Internet. A variety of network scanning tools are used to identify other rogue services
Storage			
Security of user files and resources held on School systems	Attempts to access to user's files and resources without permission	**Yes**	Access to the School's storage networks is tightly controlled by permissions based on the users' network accounts. This gives direct accountability and security

Integrity of user files and resources	Attempts to alter or delete other users' files and resources		File security makes it most unlikely that a user could maliciously damage another user's files, but in the event of such happening the ICT staff can restore from routine backups (full backups weekly and incremental backups daily of local data and daily backups of office 365 (mailboxes, OneDrive, and SharePoint. The backup regimen covers all School storage systems on a nightly basis and there are additional mechanisms to allow users to recover their own files should they become lost or damaged
Security of system and administrative resources	Attempts to access the system or School administration resources without permission		Access to the School's storage networks is tightly controlled by permission based on the users' network accounts. This gives direct accountability and security
Integrity of system and administrative resources	Attempts to alter or delete system or School administration files and resources		In addition to the mechanisms defined above all School databases are backed up to multiple locations to provide increased resilience
Unacceptable or inappropriate storage of personal data	Use of the School's storage networks in an unauthorised or insecure manner for personal data		ICT staff have access to all file systems and monitor broad patterns of use constantly. Suspicious traffic patterns are investigated in depth

Introduction of inappropriate or illegal materials onto School systems • Across the network • From other public networks • From personal devices • From removable media	The copying or downloading of inappropriate or illegal materials onto School computers or network storage solutions		The filtering software is configured to prevent access to and the downloading from Internet sites that have been categorised by the filter manufacturer. Attempts to access blocked sites are recorded and daily reports sent to the ICT Manager and his deputy
Email			
Unacceptable/inappropriate use of email	Unprofessional conduct - use of unacceptable language – inappropriate email targeting – use of school systems for commercial purposes.	**Yes**	Profanity keywords filter on emails for students
Antisocial use of email	Sending of inappropriate or unauthorised bulk emails		Moderation and approval system for sending emails to students forms and year groups.
Email attacks	Spam, mail-bombing and phishing attacks, use of botnets		Antivirus and antispam filters and can protect against a wide variety of mail-based attacks
Accidental exposure of data	Careless use of email resulting in data being send to the wrong recipient		Internal emails can be recalled by the user, and they can be deleted from mailboxes by IT. Staff induction includes advice on the careful use of email.
World Wide Web			

Access to unsuitable materials	Accessing materials and websites that are inappropriate in a school environment	**Yes**	The filtering software is configured to prevent access to and the downloading from Internet sites that have been categorised by the filter manufacturer. Attempts to access blocked sites are recorded and daily reports sent to the ICT Manager. Substantive safeguarding concerns would be reported to the Headmaster (if concerns relate to activity of a member of staff) or to the DSL (if about pupils) as per the Safeguarding and Child Protection Policy and Procedures. Concerns which are not of a safeguarding nature would be reported in the first instance to the appropriate Head of Section
Access to terrorist or extremist propaganda	Accessing or generating statements or images which endorse, condone, or incite extremist or terrorist activity		As above.
Access to illegal materials and services	Accessing child abuse materials - race or hate crime materials materials that breach the Obscene Publications Act - fraudulent or copyright materials unlicensed software or services	**Yes**	As above.

Gaming and Gambling		**Yes**	As above
Running unauthorised websites	The publicising within or outside the school of websites purporting to have official backing without permission	**Yes**	The firewalls are configured in such a way that only authorised sites and services can be publicised from the school's network to the Internet.
Social Networking			
Inappropriate or unsafe use of social media	Inappropriate communications between adults and children - exposure to grooming - awareness of audience —control of permissions - sensitivity regarding personal data - regard for reputation (school and personal)	**Yes**	Pupils are given extensive guidance through the ICT curriculum regarding the safe use of social media. Is there any key word flagging via any software?
Antisocial use of social media	Trolling, abusive messaging	**Yes**	As above
Inadequate privacy settings	Allowing public access to personal information through inadequate knowledge of security settings	**Yes**	As above

Exposure to social network-based attacks	Social engineering, fake offers, manual sharing scams, 'like' jacking, fake plugins, fake apps	**Yes**	As above
School Platforms			
Publishing of unsuitable materials	The publishing on School websites and intranets of unsuitable, inflammatory, or otherwise unauthorised materials		The school's content management solution - logs the creators and editors of content, who are identifiable through their network accounts. The webmasters for these sites have control over permissions.
Circumvention of the School's security mechanisms			
Anonymous proxies	Attempts to access websites and services otherwise prohibited.	**Yes**	Known anonymous proxies are blocked by the firewall and DNS filtering
Masquerading	Attempting to use another person's identity on the Internet – e.g. - as email sending address	**Yes**	Extensive logs are maintained on all the school's platforms that can be used forensically to trace such wrongdoing
ICT Service Issues			
Incorrectly or poorly configured systems	Security loopholes in School networks and systems because of poor design or configuration		The ICT team has a considerable range of experience in the design and maintenance of secure networks and systems. This is augmented by ongoing training and research. In addition, an external consultancy is used to provide additional support and advice.
Out of date software versions	Updates and security fixes not applied in a timely fashion		All School systems are updated at the earliest possible point - depending on on the urgency of the fix.

			Central management solutions roll out updates automatically — System Ninja RMM