HALL GREEN SCHOOL

E-SAFETY POLICY

Adopted:	8 December 2021
Next Review:	December 2023
Governing Committee:	Full Governing Body
Responsibility:	Headteacher

SECTION 1: INTRODUCTION AND KEY PRINCIPLES

The Internet is now as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing pupils and staff in embarrassing, inappropriate and even dangerous situations. This policy is designed to help ensure responsible use and the safety of pupils and staff. This e-Safety Policy is built upon the following four core principles:

1. Guided Educational Use

Significant educational benefits should result from curriculum internet use, including access to information from around the world and the ability to communicate widely and publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for forbidden activities, or activities with low educational worth.

2. Considering Risk

Internet use presents dangers including violence, racism and exploitation from which children and young people must be protected. At the same time, they must learn to recognise and avoid these risks and aim to become "internet-wise". Hall Green School must ensure that we are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils also need to know how to cope if they come across inappropriate material.

3. Responsibility

Internet safety depends on staff, schools, associates, parents/carers and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communicative technologies such as phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

4. Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation.

SECTION 2: PURPOSE, SCOPE AND REVIEW

The purpose of internet use in school is to raise educational standards, to promote Pupil achievement, to support the professional work of staff and to enhance Hall Green School's management of information and administrative systems. Internet access is an entitlement for pupils who show a responsible and mature approach to its use. The internet is now an essential tool for education, business and social interaction. Hall Green School has a duty to provide pupils with quality internet access as part of their learning experience and will include filtering appropriately tailored to the age of pupils. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Internet access will be planned to enrich and extend learning activities. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
The benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries
- educational and cultural exchanges between pupils world-wide
- cultural, vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff
- staff professional development through access to national developments, educational materials and good curriculum practice
- communication with support services, professional associations and colleagues
- improved access to technical support including remote management of networks
- cost effective use of resources
- exchange of curriculum and administration data with the LA and DfE
- mentoring of pupils and providing peer support for them and teachers.

Review period

This E-Safety policy, and linked or associated policies (such as Acceptable Use policies) have been written by Hall Green, using external and internal guidance. The Leadership Team and Governing body have agreed the Policy, and it will be reviewed every two years.

SECTION 3: ROLES AND RESPONSIBILITIES

Governors

The Governors have delegated responsibility for the E-Safety policy to the Headteacher and ICT Support Department. They remain responsible for reviewing the effectiveness of the policy.

Headteacher and Senior Leadership Team

The Headteacher is ultimately responsible for ensuring the safety (including e-safety) of members of Hall Green School. The day-to-day responsibility for e-safety will be delegated to the ICT Support Department. The Senior Leadership Team along with the ICT Support Department will ensure that there is a system in place to allow for monitoring and support of those in Hall Green School who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles which includes ICT Support Department, Heads of Year and Form Tutors. The Senior Leadership Team can receive regular monitoring reports from the ICT Support Department where required.

The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Support Department

The IT Support Department takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing Hall Green's e-safety policies. In addition, the team has the following responsibilities:

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority where appropriate
- Logging reports of e-safety incidents
- Hall Green School ICT infrastructure is secure and is not open to misuse or malicious attack
- Hall Green School meets the e-safety technical requirements outlined in the Acceptable Usage section of this document and any relevant Government E-Safety Policy and guidance
- Users may only access Hall Green School networks through a properly enforced password protection policy
- Hall Green School filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- The use of the network, including the Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse or attempted misuse is reported to the Senior Leadership Team and Governors
- That monitoring software and systems are implemented and updated. These include Smoothwall Monitoring, a system that monitors and records misuse of computing resources; Impero, a live monitoring feed to observe computer activity.

Teaching and Non-teaching Staff

Teaching and non-teaching staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Hall Green School e-safety policies and practices
- They have read and understood the ICT Acceptable Use Policy Document
- They report any suspected misuse or problem to a member of the Support Department for investigation
- Digital communications with pupils are on a professional level and only carried out using official Hall Green School systems
- E-safety issues are embedded in all aspects of the curriculum and other Hall Green School activities
- Pupils understand and follow the Hall Green School e-Safety and acceptable use procedures
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended Hall Green School activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current Hall Green School policies with regard to these devices.

In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

SECTION 4: APPROPRIATE ORGANISATIONAL STRATEGIES

This document describes organisational strategies to help to ensure responsible and safe use. They are based upon limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies are selected based upon the current situation and their effectiveness is monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant and aware of the key principles and directives to follow.

1. E-Safety lessons

In Year 7 pupils' (Term One) first Computing lessons, E-safety is covered comprehensively, together with Cyber-bullying, grooming, phishing and SMART rules. Year 8 will learn about computer viruses and network security, Year 9 pupils (Term Two) study Computing Legislation.

For KS4 pupils following the Computer Science GCSE syllabus, they will study network security, ethical issues, and computer legislation. Pupils following the BTEC syllabus will study copyright-related issues, legislation and implications of using appropriate images/content.

All pupils have to sign and return Hall Green School's Acceptable Use Policy (AUP) before access is granted. The Policy is displayed in all ICT rooms and a copy can be found on our website under School Performance\Policies with a "pupil-speak" summary of key points.

2. E-Safety- Pastoral

E-Safety along with other Personal safety issues are raised and highlighted in school Assemblies and PSHE-based form periods throughout pupils' school lives. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, and are also made aware that they can speak to any member of staff if they have concerns or are experiencing any issues.

3. E-Safety-Teaching and Support Staff

E-Safety is also covered in the ICT Whole School Policy so that staff are aware of E-Safety issues. Information on E-Safety is communicated to staff regularly, in particular with regard to Data protection and the procedures we have in place. There is an annual E-safety update during a Twilight/Teacher Day session in school where E-Safety is addressed. During this session, training will be delivered to staff in regards to the evaluation of online materials and methods of developing pupils' critical attitudes. All staff have to sign and return the agreement of acceptable use.

4. E-Safety-Parents

This E-safety overview, AUP and ICT Whole School Policy and E-Safety resources are all online for Governors, Parents, Staff and Pupils. The school also sends information out in the school newsletters to Parents who are made aware that they can contact the school if they have any concerns or issues. Please refer to our school website under School Policies.

5. E-Safety-Monitoring

As part of e-safety review at the start of each year, the ICT team reviews how effective monitoring system have been in maintaining the school network and ensuring compliance with the Acceptable Use policy in light of new technologies and current practice. Hall Green School currently utilises:

- Link2ICT
- Impero software
- Smoothwall Monitoring.

These tools monitor the following aspects:

- Content – whether a user engages with or is exposed to potentially harmful content
- Contact – whether a user, particularly a pupil, experiences or is targeted by potentially harmful adult contact
- Conduct – whether a pupil witnesses, participates in, or is a victim of potentially harmful peer conduct
- Contract – whether a pupil is party to or exploited by potentially harmful contract (e.g. identify theft).

These tools are used to monitor the integrity of the school network and ensure that all users are following the Acceptable Use Policy. Any breaches can then be referred to the appropriate person(s) and will be dealt with appropriately in line with school policies. Any necessary policy updates will follow this review.

SECTION 5: PROTOCOLS AND DIRECTIVES

1. Bring Your Own Device (BYOD)

Hall Green School does not permit users to BYOD. There are numerous examples of data and information security issues which can arise, including forgotten passwords, unpermitted access, data loss/manipulation, unwanted effects of tracking cookies and viruses/malware. Users are not permitted to BYOD and should subsequently ensure they do not attempt to connect via any hardware (and related software) that is NOT owned or supplied by Hall Green School.

Hall Green School do not accept any responsibility for the consequences of any user attempting to attach a device to our network.

2. Email

Pupils may only use official school email accounts when sending/receiving messages relating to school matters. Staff must use a school email account to communicate in their professional capacity employed by the school. As stated in the Teachers' Standards document (DfE), "*Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school*"

Pupils should not use or access personal email accounts within school, unless specifically authorised by a member of staff. Staff should only use personal email addresses on occasions where they are not contacting on behalf of, or representing the school (personal business etc.). Staff should exercise caution if using personal email addresses using the school network, as they are responsible for any associated content. This means content which appears due to being accessed via a direct and intentional attempt or via content automatically generated using tracking cookies and browsing history.

Hall Green School employs inappropriate word filtering, and where necessary can monitor any incoming or outgoing emails. Staff and pupils have an obligation to inform their line manager or (teacher) if they receive an email or other digital communication that they feel is inappropriate or if they feel uncomfortable with the message content or tone. Action will be taken in accordance with the Anti-Bullying, or other such relevant policy. In email or other digital communication, staff and pupils must not reveal their personal details or those of others, or arrange to meet anybody without specific permission.

Incoming email should be treated as suspicious and attachments not opened unless the author is known. Email from staff and pupils to external bodies is presented and controlled in the same way as a letter when written on official Hall Green School letter-headed paper. As a consequence, ensure that any communication in this format accurately represents the views of the School.

The forwarding of chain letters is forbidden.

3. Internet use

If a user is absent from school for a period of 5 days or more, or it is believed they have ceased attending Hall Green School then web based access may be disabled. Should there be any cause for concern the Headteacher may at their discretion instruct the Network Manager to suspend access.

4. Filtering

Hall Green School will work in partnership with service providers and CEOP to ensure that systems to protect students are reviewed and improved both annually and when emerging technologies dictate. Staff will have unfiltered access where appropriate to their role. Students will have filtered access as deemed appropriate by the Headteacher or the relevant Senior or Lead teacher.

Users are strictly prohibited from making any attempt to bypass or compromise the filtering and network security settings.

SECTION 6: RISK ASSESSMENT

Hall Green School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school's network. Hall Green School cannot accept liability for any material accessed, or any consequences of internet access. As a school, we will audit ICT use to establish whether the digital policy is adequate and that the implementation of the policy is appropriate and effective. This audit will form part of the policy review, and will be part of the Senior Leadership meetings.

Furthermore, the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

SECTION 7: INDUCTION AND TRAINING

Pupil induction:

All new pupils and parents/carers are asked to sign and state they have read and accepted this policy. In order to make this more accessible, the key points are summarised in a "pupil-speak" section. Rules for internet access are posted in all rooms where computers are used, and pupils are also informed that internet use is monitored. Instructions reminding pupils about responsible and safe use precedes network access every time a pupil completes the login process and the Acceptable Use section of this policy is revisited during the first term for all classes in Year 8 and above.

All Year 7 pupils complete an E-Safety module during their introductory Computing lessons.

A module on responsible internet use is included in the PSHE programme covering both school and home use.

Staff consultation and training:

All members of staff are governed by the terms of the E-Safety and Digital Policy. All staff are provided with this policy document, and its importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Staff development in safe and responsible internet use and on the key principles and directives contained within the E-Safety and Digital form part of the induction to the school and are included in the annually reviewed Code of Conduct and Handbook for all staff. As with pupil use, instruction regarding responsible and safe use will precede network access every time a member of staff completes the login process.

Enlisting Parents' and Carers' support:

Parents' and carers' attention will be drawn to the policy documents, which are accessed via our school website and issued to all new starters. Links to access this (and other related) documents will be sent via reminders at the start of every academic year. Hall Green School may also choose to issue further reminders, both individual or en masse, if necessary.

Partnership initiatives are actively encouraged, and Hall Green School will endeavour to provide the most valuable and relevant information, suggestions, links and resources via the school newsletter and/or website.

SECTION 8: RESPONDING TO INCIDENTS OF MISUSE

It is our intention that all members of the Hall Green School community will be responsible users of ICT who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or deliberate misuse.

Pupils in breach of this policy will be dealt with in accordance with the Whole School Positive Behaviour Management Policy. Any issue where staff have breached, or are suspected of breaching must be referred to the Headteacher. This can be reported directly, or via a Line Manager. Issues relating to child protection must be dealt with in accordance with Hall Green School's child protection procedures and policy document(s).

Once a concern or report of misuse is raised, the action is communicated to any relevant parties and logged against that pupil or member of staff. In extreme cases, outside authorities may be contacted as a matter of legislation or safeguarding.

SECTION 9: ILLEGAL ACTIVITY

The Headteacher or another member of the senior leadership team should be contacted urgently if any member of Hall Green staff becomes aware of, or suspects, any apparent or actual misuse of Hall Green School equipment or systems which appears to involve illegal activity. Examples of such activity include, but are not limited to:

- Child sexual abuse images
- Adult material which potentially braches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Peer on peer abuse

SECTION 10: FURTHER INFORMATION

Hall Green School feels that the best way to keep pupils safe online is through educating pupils, and communicating with pupils and parents regarding these issues. From time to time pupils may either inadvertently or intentionally try to access inappropriate material or abuse the use of ICT equipment in school and for this reason Hall Green School has a number of robust systems in place. Whilst Hall Green School ensures our systems are as robust and fit-for-purpose as possible, we strongly advise exercising restraint and applying a "safety-first" approach when using digital resources as no system will be entirely infallible. With this in mind, please be aware of the following:

- All ICT Suites are intentionally designed in such a way to aid screens being visible by staff.
- All ICT Suites have screen monitoring and capturing software where a member of Teaching Staff or a Network Administrator can view individual screens or all screens at once. Pupils not using the resource appropriately will receive a request to return to their task. If they continue and ignore the request, they will be taken off the system. At this point, the pupil will be referred to the Head of Department, Pastoral Assistant Headteacher or Senior Leadership Team
- Any inappropriate language used is also recorded and logged through software installed on all computers, and screen shots are provided and reported to Pastoral team/SLT.
- All internet traffic is filtered and logs of websites accessed by staff and pupils recorded, which can be analysed if required.
- The school makes every effort to block malicious file types.
- Any abuse of the school ICT systems by pupils is dealt with through the school's disciplinary procedures and appropriate action taken depending on the nature of the abuse. The level of action taken in case of any abuse is discussed between ICT Support Department and Head of ICT and where required, Head of House/Pastoral Team or a member of Senior Leadership Team.

APPENDIX 1: ACCEPTABLE USE PRINCIPLES AND DIRECTIVES FOR ALL USERS

When referring to "users", this list includes, but is not exhaustive:

- Teaching staff
- Leadership
- Non- teaching and cover staff
- Key stage 3 and 4 pupils
- Parents and carers
- Governors
- Third party suppliers and contractors
- Volunteers.

The following legislation must also be adhered to by all users, and underpins this Acceptable Use policy:

- Human Rights Act 1998
- Data Protection Act 1998 and General Data Protection Regulations (Effective as of May 2018)
- Freedom of Information Act 2000
- Computer Misuse Act 2000, amended by the Policy and Justice Act 2006
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Copyright, Designs and Patents Act 1988.

The following principles of acceptable use apply to all users of Hall Green School ICT systems:

- Access for staff and pupils can only be made via an authorised user account and password, which is confidential to the individual and should not be made available to any other person
- Activity that threatens the integrity of the Hall Green School ICT systems or activity that attacks or corrupts other systems is strictly forbidden. No user should attempt to access restricted files, documents, servers or applications
- Users are responsible for all emails sent, and/or contacts made that may result in email being received
- Posting anonymous messages and forwarding chain letters is forbidden
- Professional and respectful language and/or content should be applied when using Hall Green internet or email. Users should not include anything in an email that could be offensive or disrespectful
- If users discover unsuitable sites during the course of following the correct protocols and procedures, the URL (address) and content must be reported to ICT Support or any member of teaching staff immediately.
- Users should be aware that internet is 'filtered' and computer use is monitored
- Hall Green School reserves the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request
- All computers and electronic equipment must be either kept in sight of an adult or securely locked away, never left accessible to pupils without supervision
- Teachers should ensure that computers are treated well by pupils and used in a manner consistent with supporting learning (not to play games etc.)
- All faults and problems should be reported promptly to the ICT Support Department
- Equipment must be returned to ICT Support Department when required for repair, maintenance or upgrade

- Laptops and other electronic equipment are loaned for use within Hall Green School and at home when working on Hall Green business. Used must take full responsibility for the security of this equipment
- Users must not install their own software onto Hall Green School computers, unless given express permission by the ICT Support Department. Users must also ensure this software is legally authorised.

Unsuitable/inappropriate activities

- Accessing images or materials related to child sexual abuse
- Distributing criminally racist material, extremist material or promoting terrorist activity
- Cyberbullying.

are strictly prohibited from Hall Green and our associated ICT systems and could potentially lead to criminal prosecution. There is however, a further range of activities, which may generally be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. Hall Green School believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities inside or outside of Hall Green School when using school equipment or systems. Hall Green School policy restricts certain internet usage as follows:

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

- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of Hall Green School or brings the school into disrepute
- Political purposes
- Running a private business
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Hall Green School
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- 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
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- Online gaming (non-educational)
- Online gambling
- File sharing
- Use of social networking sites.

APPENDIX 2: ACCEPTABLE USE PRINCIPLES AND DIRECTIVES (PUPILS)

Access to the school network will be provided for you to carry out recognised school work only, but only on the understanding that you agree to the following guidelines.

Privacy

Computer storage areas will be treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. Users should not expect that their work and emails would always be private. You should also be aware that a member of the ICT staff can view your computer screen at anytime from anywhere on the school network without your knowledge.

Passwords and Security

- Pupils must not disclose their password to others, or use passwords intended for the use of others
- Under no circumstances should any pupil disguise, attempt to disguise or mask their identity
- Pupils must not access, copy, remove or otherwise alter other people's work.
- Pupils must not attempt to alter the settings of computers unless they are authorised to do so
- No attempt should be made to bypass or disable any anti-virus, firewall or security measures (including physical devices) in place.

Authorised use of email

The email system and the Internet area are available for communication on matters directly concerned with school business. Pupils using the email system should give particular attention to the following points:

- The standard of presentation. The style and content of an email message must be consistent with the standards that the school expects from written communications.
- The content of the email. Pupils must ensure the content of email messages sent is appropriate. Alongside inappropriate content, pupils must not:
    - use offensive or strong language
    - Use slang
    - Send irrelevant or distracting emails, especially during a lesson
- The recipient of the email. Pupils must make sure they only send emails to pupils they know. If sending to a member of staff they should have a good and valid reason.

Unauthorised use of Email

The school will not tolerate the use of the system for any of the following:

- Any message that could constitute bullying or harassment
- Personal use in school time e.g. social invitations, personal messages, jokes, cartoons or chain letters
- Downloading or distributing copyright-protected information and/or any software available to the user or others
- Sending confidential information about other pupils, school employees or the school itself.

File Storage

Pupils are responsible for files stored in their personal areas. These files should be only those related to teaching and learning (school work), careers, college applications or other aspects of their life at Hall Green School. In addition, pupils must ensure that any files copied to Hall Green School network are free from viruses.

IT Equipment (including cabling)

- Treat All equipment with care and respect so as to prevent any damage
- Do not use equipment you believe to be unsafe
- Report immediately any damage to the equipment that you become aware of
- Do not dismantle any part of the equipment (including a mouse or other peripheral device)
- Do not remove Equipment from a room or the school site without permission
- Do not relocate any piece of equipment within school unless you are asked to do so
- If you are aware of anyone damaging, stealing or misusing equipment you must report it to a teacher or senior member of staff immediately
- Do not eat or drink whilst using IT equipment
- Pupils should not connect any equipment or device to the network without the prior approval of the ICT Support Department or a member of teaching staff.

Internet Rules

1. Pupils must access the Internet only for study purposes or for school-authorised activities
2. Pupils must report accidental accessing of unsuitable sites (pupils to a teacher/teacher to the ICT Support Department)
3. Pupils are expected to respect the work and ownership rights of people outside the school as well as other pupils and staff. This includes abiding by the copyright law
4. Pupils must not engage in chat activities over the Internet. This takes up valuable resources which could be used by other people to benefit their studies
5. Pupils should never give personal information (such as their address or telephone number) to those whom they contact through email.

APPENDIX 3: ACCEPTABLE USE PRINCIPLES AND DIRECTIVES (STAFF)

Advice and guidance surrounding the use of email

The email system and the Internet area are available for communication on matters directly concerned with school business. Employees using the email system should give particular attention to the following points:

- The standard of presentation. The style and content of an email message must be consistent with the standards that the school expects from written communications. Please see clerical staff in in doubt.
- The extent of circulation. Email messages should only be sent to those employees from whom they are particularly relevant. It is not good practice to forward emails to a third party as indiscretions can often inadvertently result
- The appropriateness of the email. When and when not to use Email is a matter of individual judgement but care should be taken to ensure that it is not used as a substitute for face-to-face communication when such communication is more appropriate. "flamemails" (emails that are abusive) can be a source of stress and damage work relationships. Hasty messages sent without proper consideration can cause unnecessary misunderstandings
- The visibility of email. If the message is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The individual will be liable for any defamatory information circulated either within or to external users of the systems. Where there are concerns with the information being sent staff should check this information with senior Leadership first, by not doing this, staff could make the school liable, which could in turn mean that the school would need to invoke its disciplinary procedures in regards to the matter
- Email contracts. Offers or contracts transmitted via email are as legally binding on the school as those sent on paper. No contracts should be entered into without prior approval of the Bursar or a member of Senior Leadership Team
- Confidential content. In cases where information regarding pupils, parents or staff would be sent via email, you should consider whether the content could significantly compromise the data subject if read by another party. For example, details regarding bereavement, health, special needs or safeguarding concerns should be password protected within a word document, with a password sent separately.

Unauthorised Use

The school will not tolerate the use of the system for any of the following:

- Any message that could constitute bullying or harassment
- Personal use in school time e.g. social invitations, personal messages, jokes, cartoons or chain letters
- Personal online activity (shopping, general browsing etc.) during contact time(s) with pupils
- Accessing pornography or inappropriate images
- Downloading or distributing copyright-protected information and / or any software available to the user to others
- Posting confidential information about other employees, the school, pupils and their contacts or its suppliers.

Staff are strictly forbidden from using personal mobile or telecommunication devices for any of the above during contact time with pupils.

Privacy

Computer storage areas will be treated as school property and as such can be viewed by Administrators if required.

File Storage

Staff are responsible for files stored in their personal areas. These files should be only those related to teaching and learning or other aspects of their work at Hall Green School and must conform to the Hall Green School Data Protection policy. In addition, staff must ensure that any files copied to Hall Green School network are free from viruses.

MIS Systems (SIMS)

Staff should use these systems as required for their day-to-day work, but must not allow access to unauthorised persons. The data within these systems is likely to be confidential and staff should therefore refer to the Data Protection policy.

ICT Room Booking

Staff who wish to use an ICT room may make a booking via the Computer room booking software (**Room booking system**) and can book an ICT room up to two weeks in advance. If they require to book further in advance they will need to contact ICT Support Department. A booking more than two weeks in advance, block bookings or permanent bookings may need to be referred via the Deputy Head in charge of Curriculum. Due to the constraints of the timetable it will not always be possible to accommodate requests.

User Account creation

New staff accounts will be generated following a receipt of instructions from the PA to the Headteacher or Deputy Headteacher. Where temporary accounts are required, for example for pupil teachers or supply staff, the line manager responsible for that member of staff should make a request directly to the ICT Support Department. Issues of account security, such as requests to change passwords, should also be made to the ICT Support Department.

Resolution of Faults

Staff should report any faults or damage directly to the ICT support office. The issue will be logged in accordance with the procedures developed by the ICT Support Department and staff will be informed when the issue is resolved or is likely to be resolved. If issues are not resolved or information not provided as to when issue may be resolved, please contact the ICT Network Manager. If this still cannot be resolved, please contact the Assistant Headteacher responsible for the ICT Network.

IT Equipment (including cabling)

- Treat All equipment with care and respect so as to prevent any damage
- Do not use equipment you believe to be unsafe
- Report immediately any damage to the equipment that you become aware of
- Do not dismantle any part of the equipment (including a mouse or other peripheral device)
- Do not remove Equipment from a room or the school site without permission

- Do not relocate any piece of equipment within school unless you are authorised to do so
- If you are aware of anyone damaging, stealing or misusing equipment you must report it to the ICT Support department, and log this with the relevant Head of House or senior member of staff immediately
- Do not eat or drink whilst using IT equipment
- Staff should not connect any equipment or device to the network without the prior approval of the ICT Support Department or a member of teaching staff.

AV (Audio Visual)

Audio Visual setup can be arranged for the Hall, or other rooms by the ICT Support Department but requires 24 hours' notice (as standard).

APPENDIX 4: FURTHER GUIDANCE

Education for a Connected World
https://www.gov.uk/government/publications/education-for-a-connected-world

Cyber security - ICO https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources/#england

Teaching a broad and balanced curriculum for education recovery
https://www.gov.uk/government/publications/teaching-a-broad-and-balanced-curriculum-for-education-recovery

Sexual violence and sexual harassment between children in schools and colleges
https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

Searching, screening and confiscation at school
https://www.gov.uk/government/publications/searching-screening-and-confiscation