HALL GREEN SCHOOL

E-SAFETY POLICY
October 2016

Adopted:	10 October 2016
Next Review:	10 October 2018
Governing Committee:	Full Governing Body
Responsibility:	Mr D Adams - Headteacher
	Mrs J Owen - Chair of Governors

HALL GREEN SCHOOL

E-Safety Policy Document

Overview

Hall Green School have a number of core solutions in place to keep pupils safe in school and are continually striving to keep up with any new technology available in regards to E-Safety. To view Hall Green School Policies please refer to our school website under School Performance\Policies.

E-safety

Hall Green School recognises that new technologies have become integral to the lives of children and young people in today's society, both within Hall Green School and in their lives outside. The use of these exciting and innovative tools at Hall Green School and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside Hall Green School. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and as with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

E-Safety lessons

For upper school pupils issues are re-visited through Assemblies and Form work. Year 7 pupils (Term One) first ICT lessons E-safety is integrated with social networking and Microsoft Publisher skills together with Cyber-bullying, Bullying face to face, Hackers/viruses and SMART rules. Year 8 learn through project work, Year 9 pupils (Term Two) study Computer Laws/Microsoft Publisher. This topic is reiterated in years 10 and 11 in ICT lessons and re-visited during Assemblies. 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.

E-Safety/Pastoral

E-Safety along with other Personal safety issues are raised and highlighted in school Assemblies throughout pupils' school lives with guest speakers attending, including community support officers. Pupils are also made aware that they can speak to any member of staff if they have concerns or are experiencing any issues.

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 will be an annual E-safety update during a Twilight/Teacher Day session in school where E-Safety is addressed. All staff have to sign and return the agreement of acceptable use.

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 Students. We also send 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 Performance/Policies.

E-Safety\Monitoring

As part of e-safety review at the start of each year new technologies and current practice are examined. Policy updates follow this review.

Passwords and Security

- Staff/Students must not disclose their password to others, or use passwords intended for the use of others
- Staff must change their password in accordance with the strong password policy
- Under no circumstances should any user disguise, attempt to disguise or mask their identity
- All users are expected to respect and not attempt to bypass security in place on the computer systems
- Pupils must not access, copy, remove or otherwise alter other people's work.
- Users 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

Staff have access to the Internet to conduct their day-to-day duties. Both staff and students should ensure that their use of the Internet complies with the Acceptable Use and E-safety sections of this policy below:

Authorised Use

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

- The standard of presentation. The style and content of an e-mail 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. E-mail 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 e-mail. When and when not to use E-mail 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. "flame-mails" (e-mails 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 e-mail. 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
- E-mail contracts. Offers or contracts transmitted via e-mail 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 Management Team.

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 (e.g. on the grounds of sex, race or disability)
- Personal use in school time e.g. social invitations, personal messages, jokes, cartoons or chain letters
- On Line Gambling
- Accessing pornography or inappropriate images
- Downloading or distributing copyright 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

File Storage

Staff and students 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 Data Protection section of this policy below. In addition, staff and students must ensure that any files copied to Hall Green School network are free from viruses.

MIS Systems

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 sections on Data Protection and Information Security below

ICT Room Booking

Staff who wish to use an ICT room may make a booking via the Computer room booking software (**BOB**) 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 to 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 Office Manager or Deputy Head. Where temporary accounts are required, for example for student 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 ICT Support Department.

Resolution of Faults

Staff and students 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.

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 a teacher or senior member of staff immediately
- Do not eat or drink whilst using IT equipment
- Staff/Students 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) setup 24 hours' notice required

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

Internet Rules

1. Staff/Students must access the Internet only for study purposes or for school-authorised activities
2. Staff/Students must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive
3. Staff/Students must report accidental accessing of unsuitable sites (pupils to a teacher/teacher to the ICT Support Department)
4. Staff/Students are expected to respect the work and ownership rights of people outside the school as well as other students and staff. This includes abiding by the copyright law
5. Students must not engage in game (non-educational entertainment) activities over the internet or download such games. This takes up valuable resources which could be used by other people to benefit their studies
6. Students 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

Students should not give personal information such as their address or telephone number to those whom they contact through electronic mail.

Roles and Responsibilities

Governors

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

Head and Senior Management

The Head is responsible for ensuring the safety (including e-safety) of members of Hall Green School, through the day to day responsibility for e-safety will be delegated to the ICT Support Department. The Senior Management 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 Management Team can receive regular monitoring reports from the ICT Support Department where required.
The Head and Senior Management 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
- Liaising with ICT Support Department
- 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 Management Team and Governors
- That monitoring software and systems are implemented and updated. These include Policy Central, 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 students 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
- Students understand and follow the Hall Green School e-Safety and acceptable use procedures
- Students 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 students 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

Students

Students are responsible for using Hall Green School ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to all of Hall Green School systems. They should also:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Know and understand Hall Green School policies on the use of mobile phones, digital cameras and hand held devices
- Understand the importance of adopting good e-safety practice when using digital technologies outside of Hall Green School and realise that Hall Green School's E-Safety procedures cover their actions outside of the Hall Green School, if related to their membership of the Hall Green School.
- Part of this understanding is gained in ICT lessons at the beginning of year 7.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Hall Green School will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and VLE and will share information about national and local e-safety campaigns. Parents and carers will be responsible for:
Accessing Hall Green School website/VLE/on-line student records in accordance with the relevant Hall Green School's Acceptable Use Procedures

Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Hall Green School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital /video images to support educational aims, but must follow Hall Green School policies concerning the sharing, distribution and publication of those images and must check with the Deputy Head or Network Manager that authorisation for this has been granted by the parent/carer. Those images should only be taken on Hall Green School equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or Hall Green School into disrepute. Staff must not use mobile technology with camera or recording facilities in changing areas
- Students must not take, use, share, publish or distribute images of others without their permission

- Photographs published on Hall Green School website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images, Students' full names will not be used anywhere on a website or blog, particularly in association with photographs without permission
- Written permission from parents or carers will be obtained before photographs of students are published on Hall Green School website
- Student's work can only be published with the permission of the student and parents or carers

Acceptable use

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

- Access for staff and students 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 forbidden
- Users are responsible for all e-mail sent and or contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected. When publishing materials on the internet, Hall Green School network or virtual learning environment staff must ensure they have appropriate permission/ copyright for the number of users who will have access to it or a site/Hall Green School licence
- Posting anonymous messages and forwarding chain letters is forbidden
- The same professional levels of language and content should be applied in email as for letters or other media. Staff should not include anything in an email that they would not include in a letter or say on the telephone. Poorly written emails to external contacts can reflect a poor image of the Hall Green. Staff should use proper English and spelling in emails – not text message short cuts
- Staff should take care when addressing emails, particularly when using address groups, in order to send them only to those recipients who will have an interest or "need to know". Staff should be aware that if they use multiple addresses on email messages they send the whole list of addresses to all recipients and that this may not be advisable, or welcomed by all those recipients
- Before forwarding a received email to a third party, in some instances it may be appropriate to notify, or even seek permission from, the original sender to preserve confidentially
- Staff should take account of the Data Protection Act when considering sending personal data by email that could be linked to a named individual. It should be remembered that staff do not have absolute control over who will read their emails or who they will be forwarded to. The Data Protection Officer (the Deputy Head) should be consulted if staff have doubts about how to proceed in connection with personal data
- Staff should not use the Hall Green School email to express views or pass on material which could be construed as canvassing, lobbying, advocacy or endorsement, particularly if this is commercially or politically based and if this expresses a personal rather than Hall Green School view. If in doubt, staff should consult their line manager
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- 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 students without supervision
- Teachers should ensure that computers are treated well by students and used in a manner consistent with supporting learning (not to play games etc.)
- Teachers should ensure that pupils only use their mobile phones or other electronic devices in Hall Green School when they have express permission to do so
- 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 to staff for use within Hall Green School and at home when working on Hall Green business. Staff must take full responsibility for the security of this equipment
- Staff must only use legal, authorised software and must ensure any software they install themselves is legal. Staff must not install their own software onto Hall Green School computers, unless given express permission by the ICT Support Department.

Social Networking Sites

If staff do access social networking sites in their own time on their personal computer, the following guidelines should be adhered to in order to protect themselves:

- Do not allow current students to be recorded as a "friend" or "contact"
- If former students are allowed to be recorded as a "friend" or "contact", strictly limit their access to your profile. Former students often have friends and/or siblings who are still at Hall Green School
- Do not post personal information or contact details on such sites
- Do not post students' work on such sites
- Always consider your colleagues. Do not put your colleagues at risk by posting photos of them on your pages that could in any way be deemed to be risqué or cause them to be accused of unprofessional conduct
- Avoid networks – these can allow a wide range of site users to access your pages
- Give special consideration to groups. Your name will potentially be associated with the comments made by other site users
- Make yourself invisible (Facebook). You will still be able to contact people but students will not be able to find you should they attempt a search. On other sites such as 'myspace', lock down your pages as much as possible
- Do not voice your opinions regarding work. These sites are in the public domain. You cannot control who can see your posts on your friends' pages

Staff – personal email/websites/instant messengers

In order to protect themselves:

- Staff should not give their personal email address to students
- Staff should be careful with personal websites – students will find them and the information and pictures posted on them

Commercial, Business, Buying and Selling

All work produced using school equipment/resources is the property of the school except where express prior agreement is given by the Senior Management Team

- Staff/Students must not use the network/equipment for personal business interests unrelated to school business without prior approval
- Students must not use the network/equipment for commercial purposes e.g. to buy or sell goods or services
- Students must not use the network/equipment to sell any goods or services that are not related to normal school activity and transactions must be conducted as private individuals with full personal liability. The school accepts no liability for such activity

Unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and banned from Hall Green and all other ICT systems. Other activities e.g. Cyber-bullying is banned and could lead to criminal prosecution. There are however, a 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.

HGS 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:

- Child sexual abuse images
- 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
- Criminally racist material 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
- Using Hall Green School systems to run a private business
- Use 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
- On-line gaming (non-educational)
- On-line gambling
- File sharing

- Use of social networking sites

Responding to incidents of misuse

It is hoped 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 or irresponsible or through deliberate misuse.

Illegal activity

The Head 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

Data Protection – Data Controller – Ms G Sears

The Data Protection Act imposes statutory conditions for the maintenance of personal data on Hall Green School computer systems including Hall Green School data held on individual members of staff PCs. It is an offence to process or disclose such data if not registered to do so under the Data Protection Act. Hall Green School Staff may store personal data in respect of individual students at home for Hall Green School purposes, but such data must only be disclosed or processed in accordance with the Hall Green School Data Protection Registry entry.
The Hall Green Data Protection Policy gives details of Hall Green School obligations under the Data Protection Act. This was reviewed October 2015.

It is the responsibility of database creators to ensure that stored data is consistent with the data protection registry entry and is processed in a manner that is consistent with the data protection principles. The integrity of the system must be maintained and students should be made aware of their responsibilities.

The eight enforceable principles of good practice contained in the Data Protection Act 1998, which HGS will comply with, state that personal data must be:

- Fairly & lawfully processed
- Obtained only for one or more specified and lawful purposes
- Adequate, relevant & not excessive in relation to the purpose for which it is processed
- Accurate and kept up to date
- Not kept for longer than is necessary
- Data should be kept secure
- Not transferred to a country outside the EEC unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices:
- Personal data should only be stored on any portable computer system, USB stick or any other removable media in exceptional circumstances and with express permission from Senior Leadership but the Secure Gateway should be used to access Personal data as this means the Data doesn't leave the site and is viewed over SSL encrypted connection and Dual Factor Authentication where MIS systems are being accessed

Deputy Head attended updated training in the Data Protection Act in November 2015. All staff have Data Protection Training updated annually as part of whole school e-safety training.

If data is stored on personal school devices the following applies:

Portable devices are not allowed on the network unless authorised by the Network Manager

- The data must be encrypted and password protected
- The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, once it has been transferred or its use is complete

Disaster Planning

All Hall Green School information systems are subject to potential loss of data due to failure of software or hardware media. It is the responsibility of ICT Support to ensure that adequate backups are taken of all central Hall Green School systems. Users have the responsibility to ensure that regular back-up copies of essential data are made and stored in a safe location, remote from the system.

For information

Whilst Hall Green School feels that the best way to keep pupils safe online is through communicating with pupils on 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 have a number of robust systems in place.

- All ICT Suites are designed in such a way that it is not possible to hide what is displayed on screens easily.
- 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 accessing inappropriate software will receive a request on the screen 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 Pastoral or Senior Management Team

Important Information

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/SMT.
All internet traffic is Filtered and Firewalled and logs of websites accessed by staff and students recorded and this can be analysed if required.
The school blocks malicious file types.
Any abuse of the schools ICT systems by students is dealt with through the schools 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 Management Team.

References

E-safety websites such as BBC Bitesize\e-safety

Teach-ICT website-resources-TES\e-safety

E-safety document prepared by South West Grid for Learning/360 degrees safe

Child Online Safety Plymouth University –

www.plymouth.gov.uk/pscbesafetyuop

Ofcom Children and Parents: Media use and attitudes report 2014 –

http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf

Advice and guidance to be published 2016

www.safeinternet.org.uk/

Issues addressed by Hall Green School

Privacy issues, including disclosure of personal information
Digital footprint and online reputation
Health and well-being (amount of time spent online (internet or gaming)
Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
Copyright (little care or consideration for intellectual property and ownership – such as music and film)

http://swgfl.org.uk/products-services/esafety/resources/So-You-Got-Naked-Online
http://www.beatbullying.org/pdfs/Virtual-Violence-II.pdf