ACCEPTABLE USE POLICY

THIS POLICY IS REVIEWED ON AN ANNUAL BASIS

Policy reviewed by: Robert Bannon - Headmaster

Policy approved by: Robert Berry – Director of Operations

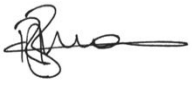
Review date: 01/09/2020

Submission:

Version: v2.0

Policy actioned from: September 2019

Next review date: 31/08/2021

Reviewer's Signature: 

Approver's Signature 

Please note: 'School' refers to Chatsworth Schools; 'parents' refers to parents, guardians and carers.

This is a whole school policy, which also applies to the Early Years Foundation Stage.

HALL SCHOOL WIMBLEDON

Contents

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Hall School Wimbledon with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Hall School Wimbledon.
- assist school staff to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying, which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- sites associated with terrorism or extreme religious or political emphasis
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking social media profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting - the act of sending sexually explicit messages or images of themselves or others, on any device that allows the sharing of media and messages. It is also referred to as SGII (Self-Generated Indecent Images or Youth Produced Sexual Imagery)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of the Hall School Wimbledon community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT systems, both in and out of Hall School Wimbledon.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside the school but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and use of electronic devices and the deletion of data. In the case of both acts, action can be taken over issues covered by the published school's Behaviour Policy and Codes of Conducts. The government guidance 'Preventing and tackling Bullying' July 2017 confirms that a staff member can examine and delete data, without parental consent, where there is good reason to do so.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
(1) Head	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. London Grid for Learning (LGfL) • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e- safety incident. • To receive regular monitoring reports from the e-Safety Co-ordinator /Designated Child Protection Lead • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager) • To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the e-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • regular review of e-safety incident logs
(2) e-Safety Co- ordinator / Designated Child Protection Lead	• To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents • To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum

	• To liaise with school ICT technical staff/consultants
	• To communicate regularly with SMT to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• To facilitate training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

(3) Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-Safety Coordinator regularly .
(4) Network Manager or Technician	• To report any e-safety related issue that arises, to the e-Safety Coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system

	• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned device • To ensure the school's policy on web filtering is applied and updated on a regular basis • To ensure that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator or Head for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures • To ensure that all data held on pupils on the server is adequately protected • To ensure that all data held on pupils on the school office machines have appropriate access controls in place
(5) Teachers.	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
(6) All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be 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 school policies with regard to these devices • To report any suspected misuse or problem to the e-Safety Coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through Continuing Professional Development • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones, social media etc.
(7) Pupils	• To read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school community

	• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-safety policies
(8) Parents /carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the Pupil Acceptable Use Agreement with their children • To access the school website in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom/ classrooms
- Policy to be part of school induction for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be signed by teachers, parents and pupils and held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

  o interview/counselling by tutor/Head of Year/e-Safety Coordinator or Head;
  o informing parents or carers;
  o removal of Internet or computer access for a period,[which could ultimately prevent

access to files held on the system, including examination coursework]; o referral to Local Authority (LA)/Police.

- Our e-Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: Behaviour Management Policy, Safeguarding Policy, Anti-Bullying Policy and Codes of Conduct.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-Safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SMT. All amendments to the policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This school

• Has a clear, progressive e-safety education programme as part of the Computing curriculum. It is built on LA / LGfL e-safeguarding and e-literacy framework for EYFS to Y6 national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

o to STOP and THINK before they CLICK

o to develop a range of strategies to evaluate and verify information before accepting its accuracy;

o to be aware that the author of website/page may have a particular bias or purpose and to develop skills to recognise what that may be;

o to know how to narrow down or refine a search;

o [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;

o to understand acceptable behaviour when using an online environment/email,i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;

o to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;

o to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;

o to understand why they should not postor share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;

o to understand why they must not post pictures or videos of others without their permission;

o to know not download any files– such as music files -without permission;

o to have strategies for dealing with receipt of inappropriate materials;

o [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;

o to understand the impact of cyberbullying,sexting and trolling and know how to seek help if they are affected by any form of online bullying.

o to know how to report any abuse including cyberbullying;

o and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

This school

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user Acceptable Use Policy, which every pupils will sign/will be displayed throughout the school/will be displayed when a pupils logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education programme;
- Provides, as part of the induction process, all new staff with information and guidance on the school's safeguarding and Acceptable Use Policies.

Parent awareness and training

This school

• Runs a rolling programme of advice, guidance and training for parents, including:

o Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear

o Information Leaflets; in school newsletters;on the school website;

o Demonstrations,practical sessions held at school;

o Suggestions for safe Internet Use At Home;

o Provision of information about national support sites for parents.

3. Expected Conduct and Incident Management

Expected conduct

In this school, all users:

o are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (Up to Year 3 it would be expected that parents/carers would sign on behalf of the pupils.)

o need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences

o need to understand the importance of reporting abuse,misuse or access to inappropriate materials and know how to do so

- o should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

- o will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- o are responsible for reading the school's e-Safety Policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- o should have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- o should provide consent for pupils to use the Internet, as well as other technologies,as part of the e-safety acceptable use agreement form at time of their child's entry to the school

- o should know and understand what the 'rules of appropriate use are and what sanctions result from misuse

All staff and pupils should be aware that the promotion of extreme political or religious ideology, whether directly or indirectly, is strictly forbidden at the school.

Incident Management

In this school:

- o there is strict monitoring and application of the e-safety policy and differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions

- o all members and its wider community are encouraged to be vigilant in reporting issues,in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

- o support is actively sought from other agencies as needed(e.g.the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues

- o monitoring and reporting of e-safety incidents takes place and contribute developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior managers and parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.

o We will contact the Police if one of our staff or pupils received online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

Contents

• Internet access, security (virus protection) and filtering

This school:

o Uses the Smoothwall,internet filtering system,which is self-managed by the school

o This system blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;

o The eSafety/Designated Lead invokes user-level filtering where relevant,thereby closing down or opening up options appropriate to the age / stage of the students;

o Ensures network health through use of anti-virus software network set-ups staff and pupils cannot download executable files;

o Uses secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off- site;

o Blocks all chatrooms and social networking sites except those that are part of an educational network or approved Learning Platform;

o Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons;

o Has blocked pupil access to music download or shopping sites–except those approved for educational purposes at a regional or national level, such as Audio Network;

o Uses security time-outs on Internet access where practicable/useful;

o Is vigilant in its supervision of pupils' use at all times,as far as is reasonable,and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

o Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;

o Ensures pupils only publish with in an appropriately secure environment:the school's learning environment

o Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age /

subject appropriate websites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , ...

o Is vigilant when conducting 'raw' image search with pupils e.g. Google Image Search;

o Informs all users that Internet use is monitored;

o Informs staff and students that they must report any failure of the filtering systems directly to the e-Safety Coordinator. Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;

o Provides advice and information on reporting offensive materials,abuse/bullying etc. available for pupils, staff and parents

o Immediately refers any material we suspect is illegal to the appropriate authorities– Police.

• Network management (user access, backup)

This school

o Uses individual,audit log-info all users-the London USO system;

o Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services

o Storage of all data within the school will conform the UK data protection requirements

Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 7 they are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far fewer security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 7.00 pm to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned; equipment installed and checked by approved Suppliers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses DfE secure websites when applicable for data transfer;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.
- We advise staff to change their passwords regularly.

E-mail
This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@hsw.co.uk
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make emails dangerous.

Pupils:

- Pupils are introduced to email use as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

  o not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;

  o that an email is a form of publishing where the message should be clear,short and concise;

  o that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;

  o they must not reveal private details themselves or others in email,such as address, telephone number, etc.;

  o to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;

  o that they should think carefully before sending any attachments;

  o embedding adverts not allowed;

o that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;

o not to respond to malicious or threatening messages;
o not to delete malicious threatening emails,but to keep them as evidence of bullying;

o not to arrange to meet any one they meet through email without having discussed with an adult and taking a responsible adult with them;

o that forwarding 'chain emails letters is not permitted.

• Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect;
- Staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

  o the sending of multiple or large attachments should be limited,and may also be restricted by the provider of the service being used;

  o the sending of chain letters is not permitted;

  o embedding adverts not allowed;

- All staff sign our HSW Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

School website

o The Head, in his absence, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

o The school website complies with the statutory DfE guidelines for publications;

o Most material is the school's own work;where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status;

o The point of contact on the website is the school address,telephone number and we use a general email contact address, e.g. enquiries@hsw.co.uk. Information or individual e-mail identities will not be published;

o Photographs published on the web do not have full names attached;

o We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

o We do not use embedded geodata in respect of stored images

Learning platform

o Uploading of information on the school's server is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

o Photographs and videos uploaded to the schools server will only be accessible by members of the school community;

o In school,pupils are only able to upload and publish within school approved and closed systems, e.g. for the purpose of completing GCSE Photography, Media Studies or Art projects;

Social networking

o Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

o We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head is the Senior Information Risk Officer (SIRO).

- Staff are clear who are the key contact(s) for key school information.

- We ensure staff know who to report any incidents where data protection may have been compromised.

- All staff are DBS checked and records are held in one central record .
  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  o staff,
  o pupils
  o parents

  This makes clear the staff's responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.

- School staff with access to setting-up usernames and passwords for email, network access are working within the approved system and follow the security processes required by those systems.

- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.

- We use the DfE S2S site to securely transfer pupil data files to other schools.

- All servers are in lockable locations and managed by DBS-checked staff.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or

restricted data has been held and obtain a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

- We are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

(*to include MP3/4 players, iPods, watches and other devices that are, or may become, web enabled devices*)

- Mobile phones and devices brought into school are entirely at the staff member, pupils', parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

- Student mobile phones, which are brought into school must be turned off (not placed on silent) and stored in the boxes provided on arrival at school. They may be collected at the end of the day. Pupils' mobile phones are stored in the school office during the day.
  All visitors are requested to keep their phones on silent.

- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of such monitoring.

- Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones when on or in the proximity of school property.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's disqualification from that examination and the overall qualification.

- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff will be issued with a school phone where contact with students, parents or carers is required (e.g. on specific trips). The school phone system should be used for all other school communication.

- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

- Mobile Phones and personally-owned devices must be switched off or switched to 'silent' mode in teaching areas. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods.

- If a member of staff breaches the school policy then disciplinary action may be taken.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use

- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

- Any images taken on school digital cameras or video cameras by staff e.g. for GCSE examinations or marketing, must be deleted once downloaded to a school marketing computer for the purpose of marketing, or managed by the Examinations Officer for submission to examination boards for marking. Images that are no longer required are either archived or deleted. Blank SD cards or other memory devices must be signed out from secure storage on each occasion that images are to be recorded. Digital recording devices and SD cards or other memory devices will be held at each school. Once downloaded to designated marketing or examination computers, all devices must be returned and signed back in to secure storage following deletion of all images.

Storage Device Disposal

SD cards or memory devices confiscated for the purpose of investigation must be returned or destroyed as appropriate once that investigation has been concluded, or when the school has been given permission to do so by the Police or other relevant authorities. Prior to return or destruction, SD cards or memory devices will be securely stored by the Safeguarding Administrator

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed.

The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix 1: Policy for the Use of Digital Images and Video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils are not referred to by name on the video, and that pupils' full names are not given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;

  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;

  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its' work in order to share its' good practice and celebrate its achievements, which is shown to other parents, schools or educators;

  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

- Your child's image being used as part of a GCSE external examination e.g.PE

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Appendix 2: Policy for the Use of Social Networking and Online Media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs,videos or any other information about them online.
- We do not write or upload' off-hand',hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload documents,photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online,and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any websites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content, which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse. The whole school community is reminded of the CEOP report abuse process:

https://www.thinkuknow.co.uk/parents/browser-safety/

All staff and pupils should be aware that the promotion of extreme political or religious ideology, whether directly or indirectly, is strictly forbidden at the school.

Appendix 3: e-Safety Agreement Form: Parents

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- o the Internet at school
- o the school's chosen email system
- o the school's online managed learning environment o
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e- behaviour they will contact me.

I understand that the promotion of extreme political or religious ideology, whether directly or indirectly, is strictly forbidden at the school.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____ Date: ___/___/___

Appendix 4: Junior Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date: ___/___/___*

Appendix 5 : Hall School Wimbledon Senior Pupil Acceptable Use Agreement

Child's Name (PRINT) _____

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not bring files into school that can harm the school network or be used to circumvent school security tools
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
6. I will only e-mail or contact people I know, or those approved as part of learning activities
7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
9. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
12. I am aware that some websites, games and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
14. I will abide by the Code of Conduct when using the Enabling Technology Room.

I have read and understand these rules and agree to them.

Signed: *Date: ___/___/___*

Appendix 6: Staff e-Safety Acceptable Use Agreement

In order to fulfil our child protection duties the school undertakes regular review and development of policies including Safeguarding, Behaviour Management, Anti-Bullying and our Codes of Conduct. In addition to the existing ICT Confidentiality and Security Policy, various new e-safety policies have been produced covering the use of social networking, online media and digital images. Your agreement to the overarching e-safety Acceptable Use Policy, which makes reference to all these policies, is now required.

Internet and ICT: I acknowledge that the school gives me access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep staff safe and to prevent staff from accessing inappropriate materials.

I understand that the school can, if necessary, check my computer files and the Internet sites that I visit at school and if there are concerns about my e-safety or e-behaviour they will contact me.

I understand that the promotion of extreme political or religious ideology, whether directly or indirectly, is strictly forbidden at the school.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I will not use personal technology to take, share (online or otherwise) or store photographs of children or staff.

I will only use school technology to take digital images and video for the purpose of promotion or evaluation of a pupil and only with prior written permission from a member of the Senior Management Team.

Social networking and media sites: I understand that the school has a clear policy on 'The use of social networking and media sites' and I support this.

Mobile Telephones: I understand and will follow school policy on the use of mobile telephones.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported, inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and at school. I will inform the school if I have any concerns.

I agree to adhere to the school's e-safety Acceptable Use Policy.

Name (PRINT) _____

Date: ___/___/___ Signature: _____

Appendix 7: Enabling Technology Room

Code of Conduct for Pupils and Staff

Welcome to the Enabling Technology (ET) Room. We hope that you will enjoy using this fabulous facility for both independent learning and taught lessons at HSW. I am sure that all users will want to apply common courtesy, common decency and common sense when using the computers. You will have access to a wide range of software and quick access to the internet on the very best computers available. Please respect them and be a responsible contributor to what could become an expanding resource for you and your colleagues. The greater the trust, the greater the freedom and the greater the opportunity for us all to enjoy.

In order to protect the interests of the school and those who understand and appreciate this resource and want to continue using it, we are proposing some rules that we should all adhere to whenever we use this room whether for computer or non-computer use. Please read and follow the rules. If you think they could be improved then please let us know. Breaking them is not an option.

All users must have read, understood and signed an Acceptable Use Policy Form before using the ET Room.

The following rules will apply at all times.

1. No food or drink is permitted in the room
2. No pupil bags or rucksacks are to be brought into the room
3. Behaviour should be exemplary at all times
4. Writing materials must not be brought into the room without permission
5. Passwords must not be shared
6. Computers, mice, keyboards and other equipment must not be tampered with
7. YOU are responsible for the computer at which you sit
8. Speakers and headphones must not be used without permission
9. USB/CD/DVD drives must only be used with permission
10. Please do not 'LOGON' until invited to do so
11. Please sit in your allocated seat. It has been selected for you for a reason
12. Never change settings or preferences on the computer unless asked to do so

Specific rules relating to the Internet: Remember that you may not:

- Use 'Chat Lines', Messenger software or Social Media Sites
- Download or install any program files
- Play games
- Fill in forms or give personal details
- Use inappropriate websites
- Communicate using inappropriate language

HSW applies web filtering and secure web gateway restrictions on all internet use. In addition, all computer and internet use is monitored by network administrators. Please do not try and test our patience.