HAYDON SCHOOL

E-SAFETY POLICY & ICT POLICY

2019

Mission Statement

- To provide all members of the community with access to appropriate ICT resources.
- To motivate and excite pupils about the possibilities that Computing and ICT has to offer.
- To produce individuals who are independent and inter-dependent users of ICT.
- To promote the use of ICT to students from all cultural backgrounds, and to use ICT for cultural enrichment.
- To produce individuals who are able to apply their understanding and knowledge of Computing and ICT successfully to novel and realistic situations, both within, and external to, the curriculum.
- To maximise the use of our ICT resources.

1. Introduction and Overview

1.1 Rationale

The purpose of this policy is to

- Set out the key principles expected of all members of the school community at Haydon School with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of Haydon School
- Assist school staff working with children 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

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

1.2.1 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
- content validation: how to check authenticity and accuracy of online content

1.2.2 Contact

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

1.2.3 Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.3 Scope

This policy applies to all members of Haydon School community (including staff, Governors, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security. Senior Information Risk Officer (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. 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 / Officer • 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)
E-Safety Co-ordinator / Designated Safeguarding Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum • Liaises with school ICT technical staff • To communicate regularly with the Leadership Team and the designated e-safety Governor / committee 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

Role	Key Responsibilities

	• To ensure that an e-safety incident log is kept up to date
	• Facilitates training and advice for all staff
	• Appropriate use of the schools' Online Learning Environment (OLE) tools namely: Show My Homework & Google Classroom
	• Liaises 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

Governors / E-safety governor	• 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. This will be carried out by the Governors Student Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
ICT Faculty Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly •
Network Manager/Technician	• To report any e-safety related issues 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 devices • The school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • 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 • That the use of the network / SIMS Parent App / Google Classroom / Remote access / email is regularly monitored in

Role	Key Responsibilities
	order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher / Year Staff 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 students on the school office computers have appropriate access controls in place • To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
SIMS Parent App	• To ensure that all data held on students SIMS for the Parent App is adequately protected
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide students carefully when engaged in acttivities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff & Governors	• 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 CPD • To model safe, responsible and professional behaviours in their own use of technology To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy • 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 • 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
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Student Acceptable Use Agreement with their children • To access the school website / SIMS Parent App / ShowMyHomework/ on-line 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
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school (See appendix 4)

1.4 Communication

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

- Policy to be posted on the school website / Google Classroom / Show My Homework / staffroom shared area / classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with students 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 held in student and personnel files

1.5 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 students are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Year Staff / E-Safety Coordinator / Headteacher
  - informing parents or carers
  - removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
  - referral to LA / Police

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

- 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

1.6 Review and Monitoring

The e-safety policy is referenced from within other school policies: Behaviour for Learning, Screen Searching and Confiscation Policy. Protocol for working with the Police and Plagiarism Policy.

- 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 Leadership Team and approved by Governors and other stakeholders. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff

2. Education and Curriculum

2.1 Student e-safety curriculum

This school:

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

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- to understand how search engines work and to understand that this affects the results they see at the top of the listings
- 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
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- 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
- to understand why they should not post or 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
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files – such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- to understand why and how some people will 'groom' young people for sexual reasons
- 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
- to know how to report any abuse including cyberbullying; 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

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student 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 students 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 students 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

2.2 Staff and governor training

This school:

- Ensures staff and Governors 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 program, CPD Programme

- Provides as part of the induction process, all new staff and governors including those on university/college placement and work experience with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

2.3 Parent awareness and training

This school offers advice and guidance for parents, including:

- introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- information leaflets; in school newsletters; on the school web site
- suggestions for safe Internet use at home
- provision of information about national support sites for parents
- parents would benefit from looking at: http://www.nspcc.org.uk/preventing-abuse/keeping-children-sate/online-safety/

3. Expected Conduct and Incident management

3.1 Expected conduct

In this school, all users:

- 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
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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
- 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 & Governors

- 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

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

Parents/Carers

- Should provide consent for students 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
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

3.2 Incident Management

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- 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
- 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
- Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders and Governors
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

4.1 Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network
- Uses the LGfL Net Sweeper filtering system which 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
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students
- Ensures network(s) healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and students cannot download executable files
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes / Internet literacy lessons
- Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Uses security time-outs on Internet access where practicable / useful
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access

- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Ensures students only publish within an appropriately secure environment : the school's learning environment – Google Classroom (G-Suite)
- Requires staff to preview websites before use (where not previously viewed or cached) and encourages use of the school's cloud based services - Google Classroom / Show My Homework as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match students' ability
- Never allows / is vigilant when conducting 'raw' image search with students e.g. Google image search; checked which are blocked
- Informs all users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the teacher. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and CPD
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA

4.2 Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the London USO system
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies
- Storage of all data within the school will conform to the UK data protection requirements

Students 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. We also provide a different / username and password for access to our school's network
- Staff access to the schools' management information system is controlled through a separate password for data security purposes

- We provide students from Year 7 with an individual network log-in username and password
- All students have their own unique username and password which gives them access to the Internet, Network Drives (shared Resources), the Google Classroom, Show My Homework and their own school approved email account
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for students and one for staff. Staff and students 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. Users needing access to secure data are timed out after 10 minutes and have to re-enter their username and password to re-enter the network
- Requests that teachers and students 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 after 5pm 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
- 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
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved suppliers / LA electrical engineers
- 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: LGFL remote access RAV3 system
- 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 or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child

- Provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their username and password (their USO username and password) – Google Classrom
- 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 our broadband network for our CCTV system and have had set-up by approved partners
- Uses the DfE secure s2s website for all CTF files sent to other schools
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX)
- 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

4.3 Password policy

- This school makes it clear that staff, governors and students must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff and governors have their own unique username and private passwords to access school systems. Staff and governors are responsible for keeping their password private
- We require staff and governors to use passwords for access into our MIS system
- We require staff and governors to change their passwords into the LGfL USO site, every 90 days

4.4 E-mail

This school:

- Provides staff and governors with an email account for their professional use, London Staffmail / LA email and makes clear personal email should be through a separate account
- Provides highly restricted (Safe mail) Uses Londonmail with students as this has email content control
- Does not publish personal e-mail addresses of students, staff or governors on the school website. Staff school email addresses are available via the school website. We use info@haydonschool.org.uk for communication with the wider public
- Will contact the Police if one of our staff, governors or students 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 e-mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product RM Virus Protect (Symantec Antivirus), plus direct e-mail filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web

4.5 Students

- We use LGfL LondonMail with students and lock this down where appropriate using LGfL SafeMail rules
- Students' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection
- Students are introduced to, and use e-mail as part of the ICT/Computing scheme of work
- Students can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this
- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail 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
  - that an e-mail is a form of publishing where the message should be clear, short and concise
  - that any e-mail 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
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
  - that they should think carefully before sending any attachments
  - embedding adverts is not allowed
  - 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
  - not to respond to malicious or threatening messages
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
  - that forwarding 'chain' e-mail letters is not permitted

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

4.6 Staff & Governors

- Staff and governors use the LGfL e-mail systems from any internet connection
- Staff and governors only use LGfL e-mail systems for professional purposes
- Access in school to external personal e-mail accounts is blocked
- Staff and governors use a 'closed' LGFL e-mail system which is used for LA communications and some 'LA approved' transfers of information
- Never use e-mail to transfer staff, governor or student personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, named LA /LGFL system
- Staff and governors know that e-mails 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'
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
  - the sending of chain letters is not permitted

- embedding adverts is not allowed

- All staff and governors sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with

4.7 School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers: e.g. R Dixon administration officer
- The school web site complies with the statutory DfE guidelines for publications
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@haydonschool.org.uk
- Photographs published on the web do not have full names attached
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website
- We do not use embedded geodata in respect of stored images

4.8 Online Learning Environmnet (OLE): Google Classroom / Show My Homework

- Uploading of information on th**e** schools' OLE is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the schools OLE will only be accessible by members of the school community
- Students are only able to upload and publish within school approved and closed system, Google Classroom
- Students who abuse other students or post inappropriate materials will in the first instance be issued with a detention for a minor offence. For more serious offences or if they continue to post and write inappropriate comments, they will be issued with a sanction by the Year Office. This could include time in isolation or an exclusion

4.9 Social networking

- 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
- The school's preferred system for social networking will be maintained in adherence with the communications policy via LGfL mail/school twitter account used for school work
- Staff must ensure that any comments they write into forums or message boards are appropriate and do not cause offence. If a member of staff opens a forum or message board they should check to ensure that the content is appropriate

School staff will ensure that in private use:
- No reference should be made in social media to students, 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 /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.10 Video Conferencing

This school
- At present the school does not make use of video conferencing

4.11 CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. Please refer to the CCTV Policy.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes

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

5.1 Strategic and operational practices

At this school:
- The Head Teacher is the Senior Information Risk Officer (SIRO)
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet
- 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 on SIMS
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed
  - staff
  - governors
  - students
  - parents – for SIMS Parent App
  - Volunteers & guests

This makes clear staffs' 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 require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. 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 e-mail, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored

5.2 Technical Solutions

- Staff have a secure area 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 encrypted flash drives if any member of staff has to take any sensitive information off site
- We use the DfE S2S site to securely transfer CTF student data files to other schools
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution
- We use LGFL RAv3 / VPN solution with its 2-factor authentication for remote access into our systems
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children
- We use the LGfL secure data transfer system, USO AutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area
- All servers are in lockable locations and managed by authorised DBS-checked staff
- We lock any back-up tapes in a secure, fire-proof cabinet
- We use LGfL's GridStore remote secure back-up for disaster recovery on our network admin, curriculum servers
- 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 get 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

6. Equipment and Digital Content

Staff are responsible for using school mobile devices including i-pads, these should only be used for school work

6.1 Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated on the school site, and signs to this effect are to be displayed throughout. Specifically in the canteen and outside during break and lunchtime
- Mobile phones brought into school are entirely at the staff member, governor, students' & 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 out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Students may use their phones at break and lunch in designated areas. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary
- 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 routine monitoring
- Where parents or students need to contact each other during the school day, they should do so only via the School's telephone. Staff may use their phones during break times
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices
- 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 will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff
- 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
- Personal mobile phones will only be used during lessons with permission from the teacher
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned

6.2 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 student 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. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- If a student 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
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences
- Students should not pass a mobile phone number on to a third party

6.3 Staff and governor use of personal devices

- Staff and governor handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day
- Staff and governors 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
- Staff and governors will be issued with a school phone where contact with students, parents or carers is required
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team
- Staff and governors should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose
- If a member of staff or governor breaches the school policy then disciplinary action may be taken
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- Use of a personal device on Haydon grounds constitutes acceptance of the Haydon E-Safety Policy, without Exception. The device needs to have its own anti-virus software

6.4 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 students in online photographic materials or include the full names of students 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 students
- If specific student photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Students are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work

- Students 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
- Students 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

6.5 Asset disposal

- Details of all school-owned hardware will be recorded on an online based school asset management system
- Details of all school-owned software will be recorded in a software 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.

7. How and where is ICT currently being used?

An audit will be carried out on a regular basis to find out where computing is being used across the school. It will be the responsibility of the Lead Teacher for the Google Classroom and ICT Faculty Reps to map ICT use in each faculty. The Lead Teacher will gather this data together to produce a whole school map of ICT use.

8. How will ICT be delivered to students?

8.1 All students in Years 7 and 8 have a one ICT lesson each week. At Key Stage 4 computer science and iMedia are options, so students will have five lessons per two weeks.

8.2 In addition to this all areas of the curriculum will make appropriate and effective use of ICT to enhance the delivery of their curriculum.

9. How will pupil's progress be recorded?

9.1 A central record will be kept to show individual progress. Teachers may of course record more data than this in their individual mark books. This will include progress made by each ethnic group.

10. How will access to ICT resources be managed?

10.1 The school has 16 full ICT suites. Additionally over 19 smaller ICT suites.

10.2 These rooms can be booked by teachers when there are no scheduled classes. All room booking is made through the support staff dealing with cover.

10.3 Pupils should not be sent to ICT rooms unless the member of staff responsible is willing to supervise the pupils.

10.4 Supervised access to rooms: 84 before school and 82 and/or 84 after school.

11. How will resources be purchased and maintained?

11.1 Any plans to purchase hardware and/or software should be discussed with the Deputy Headteacher responsible for ICT, the Network Manager and emailed to itsupport@haydonschool.org.uk

11.2 The Network Manager and ICT technicians are responsible for the everyday maintenance of the curriculum computers.

11.3 Staff must report faults with hardware and software using either of the methods outlined below, but preferably using the first two methods (please state your name, location of computer equipment, brief description of fault).

1. Email to: itsupport@haydonschool.org.uk

2. Telephoning ICT Office on extension: 120.

3. For emergencies - Telephone the Network Manager on extension: 151.

12. How will the issue of software copyright and the data protection act be dealt with?

12.1 School software and licencing information is stored centrally in the ICT office (room 86). It is also stored electronically in a central folder called ITDoc on the main school server (Hay-sr-001).

12.2 All data storage will comply with the data protection act. It will be the responsibility of the member of the Leadership Team with responsibility for ICT to make sure that the data registrar is kept informed.

13. Who assesses staff needs and delivers INSET?

It is the responsibility of the member of the Leadership Team for professional development along with the Faculty Manager and the individual who is responsible for the Performance Review to assess and evaluate staff ICT training needs. The Lead Teacher for the Online Learning Environment and any other staff who have the requisite skills will deliver INSET. External organisations will be used where this is deemed appropriate.

14. Who is responsible for implementation of ICT policy?

It is the role of the member of the Leadership Team responsible for ICT strategy in conjunction with the ICT Manager to oversee the implementation of ICT policy.

15. Who will be responsible for monitoring, reviewing and changing the policy?

The member of the Leadership Team responsible for ICT strategy, the Lead Teacher for the OLE and the Head of Computing are responsible for monitoring the policy. They must evaluate the effectiveness of the policy and negotiate with staff changes according to need. The whole policy will be re-evaluated regularly. The member responsible for ICT strategy will determine priorities, in discussion with the Leadership Team, Governors and the Head of Computing.

16. Internet Use

16.1 Why is Internet access important?

- The purpose of Internet access in our school is to raise educational standards, to support the professional work of staff and to enhance the school‘s management information and administration systems.

- Access to the Internet is a necessary tool for staff and students. It is an entitlement for students who show a responsible and mature approach to its use.

Appendix 1

Haydon School
Acceptable Use Agreement – Student

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

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
3. I will only edit or delete my own files and not view, or change, other people's files without their permission.
4. I will keep my logins, IDs and passwords secret.
5. I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
6. I will not visit inappropriate web sites such as those that exhibit pornography, sexism, racism, extremism or homophobia.
7. I will only e-mail people I know, or those approved by my teachers.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
10. I will not give my home address, phone number, send photographs 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.
11. I will never arrange to meet someone I have only ever previously met on the Internet or by e-mail or in a chat room, unless I take a trusted adult with me.
12. 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 save it and talk to a teacher / trusted adult / the Year Office.
13. I am aware that some websites and social networks have age restrictions and I should respect this.
14. 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.
15. I understand that the school may check my computer files and may monitor the Internet sites I visit
16. I agree that if I fail to follow the guidelines outlined above, my access to the Internet and/or the school computer network will be removed.

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

Signed: ……. Date: …….

Name: …… Form: ……

Appendix 2

Haydon School
Acceptable Use Agreement – Parent

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:

- the Internet at school
- the school's chosen e-mail system
- the school's online Cloud system Google Classroom (G-Suite)
- 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.

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.

Student name: ..... Form: …….

Parent / guardian signature: .....

Date: .....

PARENTAL CONSENT FOR WEB PUBLICATIONS OF WORK AND PHOTOGRAPHS

I agree that, if selected my son/daughter's work may be published on the school Web site. I also agree that photographs and video that include my son/daughter may be published subject to the school rules and that photographs will not clearly identify individuals and that full names will not be used.

Signature .....Date .....

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 aren't referred to by name on the video, and that pupils' full names aren't 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 or videoed (by the teacher, teaching assistant or other pupil) using only school technology as part of a learning activity; e.g. to analyse practical skills in PE lessons
- 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.

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.

The use of social networking and on-line 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, extremist 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 comments, 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 web sites 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 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/

Appendix 3

Haydon School
Acceptable Use Agreement –
All Staff, Volunteers and Governors

These rules cover the use of all digital technologies in school: i.e. e-mail, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the separate e-safety policy (including mobile and handheld devices).
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems, or any other / Local Authority (LA) system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network / information security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school approved e-mail system for any school business, including communication with parents. This is: LGfL StaffMail. I will only enter into communication regarding appropriate school business. Professional language must be used in all emails.
- I will only use the school's approved systems: LGfL London Mail / Google Classroom to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the Network Manager.
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's Sophos anti-virus and other ICT 'defence' systems.
- I will not record images or videos of pupils or staff without their permission.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff shared area.
- I will follow the school's policy on use of mobile phones / devices at school and will not take into classrooms / only use in staff areas / only use during break times.
- I will use the school's Online Learning Environment (OLE) in accordance with school protocols (Show My HomeWork / Google Classroom) etc.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities, and that I will notify the school of any "significant personal use", as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the LGfL / school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. (Information sharing March 2015)
- I will alert the Designated Safeguarding Lead if I feel the behaviour of any child may be a cause for concern.
- I will only use any other/LA system I have access to in accordance with its policies.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff, volunteers, visitors, governors, guests or pupils), which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead/Headteacher.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Headteacher /Designated Safeguarding Lead on their request.
- Staff that have a teaching role only: I will embed the school's e-safety / digital literacy curriculum into my teaching.

Acceptable Use Agreement Form: Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job Title / Role .....

Authorised Signature / Head/Deputy / Senior Teacher (Secondary)

I approve this user to be set-up on the school systems relevant to their role.

Signature ..... Date .....

Full Name ..... (printed)

Appendix 4

Haydon School Guest WIFI Acceptable Use Policy

By connecting to the Haydon School WIFI network you agree to the following usage policy:-

- You agree and accept that the wireless service is used at your own risk.
- You agree and accept that your equipment is used at your own risk.
- You agree and accept that no technical support will be provided.
- You agree and accept that this wireless service will not be misused. Examples of misuse include but are not limited to:
    - Fraud & theft
    - System Sabotage
    - Introduction of viruses, Trojans, malware, spyware and time bombs
    - Obtaining unauthorized access to any services
    - Breaches of Software Licensing Copyright Act, Computer Misuse Act, or Data Protection Act
    - Sending abusive, rude or defamatory messages via email, IRC or any other means
    - Accessing pornographic web sites
    - Transmission of unsolicited advertising
    - Hacking or attempted hacking
    - Disabling or overloading any school computer systems or network, or circumventing any system intended to protect the privacy or security of another user
    - You will not disseminate the WIFI logon details to anyone

- You agree and accept that any information sent or received is sent as clear text and maybe intercepted and WIFI usage monitored.
- Haydon School Internet facilities and computing resources must not be used to violate the laws and regulations of the UK or any other nation.
- Haydon School will co-operate with any legitimate law enforcement activity to prevent and/or detect illegal activities.
- You agree and accept that any misuse will result in premature termination of services with no refund, and may result in prosecution.

Signature Date

_____ _____

First Name Surname

_____ _____

Organisation Name

_____

History

Date	Issue	Status	Comments
April 2015	1	New	To Student Committee 19.05.15. Approved with noted amendments. To Governors for final approval by email 03.06.15. Approved by email 08.06.15
June 2019	1	Merged Document	Merged E-Safety Policy and ICT Policy. K Bagga Remove reference to SIMS Learning Gateway with SIMS Parent App and Show My Homework. K Bagga. To student committee 27.06.19. Approved. To FGB 11.07.19. for info only.