HOE VALLEY SCHOOL
E-SAFETY POLICY

Person Responsible	Deputy Head
Date Adopted	September 2015
Date of last review	April 2019
Date of next review	Autumn 2022

To be read in conjunction with the Acceptable Use Policy and Child Protection & Safeguarding Policy

> *"Schools are responsible for day-to-day health and safety whenever your child is in the care of school staff - this includes school trips and clubs"* ***Department for Education***

1. OUR VALUES

As a school we believe that E-safety is paramount to the general safety of all students. HVS is a Google school which uses ICT as an enabler for all lessons, and as such e-Safety is an important element of the operation of the school. All staff and governors are committed to working with students and parents in supporting students' safety and welfare in order to achieve the best possible outcomes for all. This is achieved by providing a secure and caring learning environment, which allows students to flourish in the knowledge that they are in a safe place and, should they have any concerns about their safety, they know who to speak to about it.

2. AIMS

- To set out the key principles expected of all members of the school community at HVS with respect to the use of ICT-based technologies
- To safeguard and protect the children and staff of HVS
- To 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
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- To have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- To 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

3. OBJECTIVES

At HVS, 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.

3.1 For students

- To read, understand, sign and adhere to the Student 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
- 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
- To take part in the annual 'Internet Safety' online survey

3.2 For parents and 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 / MIS / SIMS / on-line student records in accordance with the relevant school Acceptable Use Policy
- To consult with the school if they have any concerns about their children's use of technology

3.3 For teachers and form tutors

- To embed e-safety issues in all aspects of the curriculum and other school activities
  To ensure e-safety forms part of the PSHE and Computer Science
  To supervise and guide students carefully when engaged in learning activities involving online technology (including, enrichment and extended school activities if relevant)
- To make students aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

3.4 For all staff including external providers

- To read, understand and help promote the HVS e-safety policies and guidance
- To read, understand, sign and adhere to the HVS Acceptable Use Agreement
- 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.

3.5 For Deputy Head Teacher (E-Safety Co-ordinator and DSL)

- 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 technician and receive weekly Impero Reports to monitor students' online behaviour
- To communicate regularly with the Head Teacher and the Designated Safeguarding Leads 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 if appropriate
- To ensure that the school 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

3.6 For Head Teacher

- 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
- 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 ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (Senior I.T. Technician)
- To ensure that all school computers and/or cloud-based systems which hold or have access to data held on students have appropriate access controls in place

3.7 For the Board of Governors

- To ensure that the school follows all current e-safety advice to keep the students and staff safe
- To regularly review the effectiveness of the E-Safety policy. This will be carried out by the Learning and Development Committee which will receive regular information about e-safety incidents and will monitor reports. The Safeguarding governor will also monitor e-Safety and report back to governors on a termly basis.
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities
- The Safeguarding Governor will regularly review the operation of the policy with the Senior I.T. Technician (including e-safety incident logs, filtering / change control logs

4. COMMUNICATION

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

- Policy to be posted on the school website and available to all staff on the School network. Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with and signed by students at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Staff Acceptable use agreements to be held on file

5. HANDLING COMPLAINTS

HVS 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 device. The school cannot 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 form tutor / Head of Personalisation Senior I.T. Technician / Head Teacher
    - informing parents or carers
    - removal of Internet or computer access for a period
    - referral to LA / Police
- Our Senior I.T. Technician acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the Child Protection & Safeguarding policy.

6. EDUCATION AND CURRICULUM

HVS has a clear, progressive e-safety education programme as part of the Computer Science curriculum and PSHE curriculum. 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
- For older students, 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
- For older students 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
- Plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- To 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
- Ensure staff model safe and responsible behaviour in their own use of technology during lessons

- Ensure 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

7. STAFF AND GOVERNOR TRAINING

HVS:

- 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 program; annual updates/ weekly briefings
- Provides, as part of the induction process, all new staff [including on teacher training placement with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies

8. PARENT / CARER AWARENESS AND TRAINING

HVS runs a rolling programme of advice, guidance and training 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
- "Fast Forward" evening for Year 7 parents in their first half term on joining HVS
- Demonstrations, practical sessions held at school
- Suggestions for safe Internet use at home
- Provision of information about national support sites for parents

9. INCIDENT MANAGEMENT

At Hoe Valley 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 of staff and the wider school 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/the School's appointed IT partner as needed in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents takes place and contributes 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

10. MANAGING THE ICT INFRASTRUCTURE

10.1 Internet access, security (virus protection) and filtering

- HVS is using Sonic Wall to filter broadband traffic by user type. Sonic Wall's Content Filtering Service (CFS) 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
- CFS integrates "proxy avoidance" countermeasures to prevent students from circumventing associated controls and engaging in potentially unlawful or unsafe web-based activities
- E-Safety monitoring will be provided by Impero. Impero simultaneously monitors and logs all student devices, including visited websites, attempts to visit blacklisted websites and all Windows activity.
- Ensuring network health through use of SonicWall firewall (from Joskos) and network set-up so staff and students cannot download and install executable files;
- Using Egress 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;
- Blocking all chat rooms and social networking sites except those that are part of an educational network or the school's Google domain;
- Using security time-outs on Internet access where practicable / useful;
- Working in partnership with Joskos to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- 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;
- Ensuring students only publish within an appropriately secure environment: the school's Google domain / or secured network.
- Use of Google safe search.
- Monitoring all internet use.
- Immediately referring any material we suspect is illegal to the appropriate authorities e.g. the Police.

10.2 Network Management (user access, backup)

Hoe Valley School

- Uses individual, audited log-ins for all users
- 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;
- Has additional local network auditing software installed;
  Ensures the Systems Administrator / network manager is up-to-date with Joskos services and policies / requires the Technical Support Provider to be up-to-date with Joskos 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 General Data Protection Regulations (GDPR) where storage is hosted within the EU.

To ensure the network is used safely, HVS:

- 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 SIMS is controlled through a separate password for data security purposes;
- Requires all students to have their own unique username and password which gives them access to the Internet and their own Google 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
- Has set-up the network with a shared work area for staff only. Staff and students will store their teaching and learning materials and work in Google
- Has set-up the network so that users cannot download executable files / programmes remotely
- 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 any laptop or other device 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
- Has set up access permissions in Google and SIMS to ensure staff only have access appropriate to their role
- Ensures that access to the school's network resources from remote locations by staff is via Remote Desktop Software.
- 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 SIMS Support
- Provides students and staff with access to content and resources through Google Apps for Education which staff and students access using their username and password
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data
- Uses the DfE secure s2s website for all CTF files sent to other schools
- 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

10.3 Password Policy

- The school makes it clear that staff 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 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 a long password -8 letters- containing both numbers and letters.

10.4 E-mail

Hoe Valley School:

- Provides staff with an email account in Google Apps for Education for their professional use and makes clear personal email should be through a separate account
- Does not publish personal e-mail addresses of students or staff on the school website. We use anonymous or group e-mail addresses, for example info@hoevalleyschool.org / head@hoevalleyschool.org / for communication with the wider public
- Will contact the Police if one of our staff 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 emails dangerous

Students are:

- Introduced to Google Classrooms as part of the ICT/Computing scheme of work and are shown how to communicate with one another using the 'comments' button.
- Taught about the safety and 'etiquette' of using e-mail d at home i.e. they are taught not to give out their e-mail address unless it is to someone they know and trust and is approved by their teacher or parent/carer
- Told that an e-mail is a form of publishing where the message should be clear, short and concise. They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
- Told 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 and embedding adverts is not allowed
- Told 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 and not to respond to malicious or threatening messages
- Told not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
- Told not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
- Told that forwarding 'chain' e-mail letters is not permitted

Staff are :

- Told only to use the G-Mail, or SIMS email systems on the school system
- Told that access in school to external personal e mail accounts may be blocked
- Told not to use email to transfer staff or student personal data. We use the Egress system for such transfers and the google drive for storage.
- Staff know that e-mail 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.
- Told that the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
- Told that the sending of chain letters is not permitted
- Required to sign our Acceptable Use policy 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.

School website:

- The Head Teacher 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 authoriser: Tracy Wright
- 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@hoevalleyschool.org. Home information or individual e-mail identities will not be published
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website

Google Apps for Education

- Uploading of information into the school's Google domain 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 Google domain will only be accessible by members of the school community
- In school, students are only able to upload and publish within school approved systems such as Google

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

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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They comply at all times with the school's Social Media policy

Video Conferencing HVS

- Only uses skype for video conferencing activity
- Only uses approved or checked webcam sites

CCTV

- We may 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

11. DATA SECURITY: MANAGEMENT INFORMATION SYSTEM ACCESS AND DATA TRANSFER

11.1 Strategic and operational Practices

At this school:

- The School have an external Data Protection Officer (DPO)
- 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 a Single Central Register which is a secure private document.
- 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
- School staff with access to setting-up usernames and passwords for email, network access and Google/SIMS 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

11.2 Technical Solutions

- Staff have secure area(s) in Google to store sensitive documents or photographs
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 5 minutes idle time
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools
- We use the Pan-Surrey Admissions system (based on USO FX) to transfer admissions data

- We use Egress email system to transfer other data to schools in London, such as references, reports of children
- We store any Protect and Restricted written material in lockable storage cabinets
- All servers are in lockable locations and managed by DBS-checked staff
- We use the JKloud service for remote backup of the network storage. Google and SIMS are cloud based services that are backed up by the operators of the service
- Paper based sensitive information is <shredded, using cross cut shredder / collected by secure data disposal service.

12. EQUIPMENT AND DIGITAL CONTENT

12.1 School mobile devices including chromebooks, tablets and laptops

- The school provides chromebooks, laptops and tablets for the use of students during the school's extended day. The laptops and tablets are setup by the school's IT provider and designed to tie access to the school's network ensuring appropriate e-safety protection and monitoring
- Student devices will be managed by the school and will not be allocated to individual students, or provided to the students to take home with them
- The school provides laptops or chromebooks for all teachers and teaching support staff. The devices are setup by the school's IT provider and designed to tie access to the school's network ensuring appropriate e-safety protection
- The school has a camera for taking photographs of school visits and events, and to be used as part of the students' multi-media project work. The camera is managed by the Marketing and Events Co-ordinator who will ensure that content from the camera is only uploaded into the school's network.

12.2 Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, 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 in school bags before arrival to school. They must remain turned off and out of sight until the end of the day.
- 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 Head Teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Teacher 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 through the School's telephone. Staff may use their phones during non-teaching times away in staff areas or offices only.
- 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
- No images or videos should be taken on mobile phones or personally-owned mobile devices

12.3 Students' use of personal devices

- 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

12.4 Staff use of personal devices

- 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
- Staff will be issued with a school phone where contact with students, parents or carers is required
- 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 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 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

12.5 Digital Images and Video

At HVS, 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 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 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 pupil 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

12.6 Asset Disposal

- Details of all school-owned hardware are recorded in a hardware inventory
- Details of all school-owned software are 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.