HENLEY-IN-ARDEN SCHOOL

Achieving Excellence Together

Name of Policy	**E-Safety Policy** **(Online Safety, Internet and Acceptable Use of IT Policy)**	
Lead	Mr J Roper, Headteacher	
Governor Committee	Chair of Governors	
Policy Status	Updated	October 2024
	Governor Approved	Yes
	Date Governor Approved	November 2024
Review Frequency	2 Years	
Next Review	September 2026	

Table of Contents

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. 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 academy 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 Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the BSII Committee receiving information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Pastoral Link Governor. The role of this Governor will include:

- Meetings with the Designated Safeguarding Lead
- Monitoring of any online safety incident logs
- Reporting to relevant Governors Committee meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead (DSL) and Network Manager.

- The Headteacher and the DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents).
- The Headteacher / Senior Leaders are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team / Senior Management Team will receive required monitoring reports from the DSL and/or Network Manager.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

DSL - Online Safety Coordinator:

- Takes responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Meets with Pastoral Link Governor to discuss current issues, review incident logs and filtering
- Reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / Technical Staff ensures:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- the security of the school information systems will be reviewed regularly
- that the academy meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- that local and network virus protection will be regularly updated
- that system capacity will be reviewed regularly
- that use of users logins and passwords to access the school network will be enforced
- confidential data sent over the internet or taken offsite will be encrypted
- the filtering policy is applied and updated on a regular basis.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader / DSL for investigation / action / sanction
- that servers must be securely located and physical access is restrained
- that monitoring software / systems are implemented and regularly updated
- that the server operating system must be secured and up to date

- that access to wireless networks must be proactively managed and secured with a minimum WPA2 encryption.
- that new cloud based systems for students, students and carers are rigorously tested before implementation and check they are secure and protected. Reasonable levels of support are provided to parents to confirm they can access these services from their personal devices. (E.g. School Gateway, seneca, Office365). The school cannot accept responsibility for solving issues on non-school devices.
- emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- any computers or storage media that may have held personal or confidential data must have their hard drives secured erased either before or as part of the disposal process. This is the ensure compliance with the data protection act.
    - Under the Waste Electrical and Electronic Equipment regulations (WEEE) the Academy will only use registered WEEE authorised agencies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy E-Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the *Headteacher / Senior Leader / DSL / Network Manager* for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- they inform and educate students about the risks associated with taking, use, sharing, publication and distribution of images, in particular they should recognise the risks of publishing their own images on the internet (e.g. publishing images on social media sites).
- digital/video images taken to support education aims follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment. The personal equipment of staff should not be used for such purposes.
- care be taken when taking digital/video images and that students are appropriately dressed and are not participating in activities that may bring the individuals or academy into disrepute.

- concerns regarding students use of social networking, social media, and personal publishing sites (in or out of schools) be raised with their parent/ carers, particularly when concerning students underage use of sites.
- official blogs or Wiki's be password protected and run from the school website with the approval of the senior leadership team. Members of staff are advised not to run social network spaces for students use on a personal basis.
- social media tools used with students as part of the curriculum are risk assessed before use and the sites terms and conditions are checked to ensure it is age appropriate. Staff will obtain documented consent from the senior leadership team before using social media tools in the classroom.
- where video conferencing is used as part of the curriculum:
    - Online tutors have a clean enhanced DBS provided to the school on request or students must be monitored by a member of the Academy staff for the full duration of the video conference. It is recommended sessions should be recorded and written permission should be given by all sites and participants. The reason for the recording must be give and should be clear to all parties at the start of the conference). No contact would be allowed outside of the conference session. Video conference tutors would only know the students first name, no surname, school name or location.
    - All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
    - Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Students:

- Are responsible for using the academy digital technology systems in accordance with the Responsible Use of ICT by Students Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital devices.
- Must not take, use, share, publish or distribute images of others without their permission. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues where possible. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Endorsing by signature the student acceptable use of ICT policy
- Digital and video images taken at school events
- Access to parents' sections of the website / Learning Platform and on-line student / pupil records
- Their children's personal devices in the academy (where this is allowed)
- Ensuring that they themselves do not use the internet / social network sites / other forms of technical communications in an inappropriate or defamatory way.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside academy.
- Students should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would

normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Students will be advised to never give out personal details of any kind which may identify them or their location.
- Students will be advised on security and privacy online and will be encourages to passwords, deny access to unknown individuals and to block unwanted communications.
- Students are advised not to publish specific and detailed private thoughts, especially those which may be considered threatening, hurtful or defamatory.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Kindness Week
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff on request.
- All new staff should receive online safety information as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- This Online Safety Policy and its updates will be presented to staff and discussed by staff in team meetings when appropriate.
- The DSL will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered via participation in academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers and wireless systems must be securely located and physical access restricted (as much as physical building restraints allow).
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and password (users are required to create a secure password during initial login) by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "master / administrator" passwords for the academy ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure location.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Requests made for filtering changes for students must be authorised by the Head teacher or DSL
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced / differentiated user-level filtering
- Academy technical staff are able to monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report technical or security issues to the Network Manager.
- Filtering is not 100% effective, there are ways to bypass filters and it is therefore important that students are supervised when using internet access and that acceptable use polices are in place.
- Any material that the school believes is illegal will be reported to the appropriate agencies.
- If staff or students discover unsuitable sites, the URL will be reported to the Network Manager who will action the concern as appropriate.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- A process is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

Applications for temporary access are made to the Network Manager who authorises appropriate time limited access.
- An agreed policy is in place that forbids staff from installing unauthorised software or hardware on school devices.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's cloud based services such as email and data storage.

Pupils are **not** permitted to use their own smart phones during school hours (from 8:30 am to 3:15 pm). These devices must be switched off (not just in "Silent" or "Airplane" mode) and should be out of site and reach at all times. Sanctions which will be put in place if these rules are broken are outlined in the school's behaviour policy.

All users should understand that the primary purpose of the use mobile / personal devices in school or to access school resources remotely, is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education program.

- The school Acceptable Use Agreements for staff and students/students will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	✓	✓	✓			
Full network access	✓	✓				
Internet only			✓			
No network access				✓	✓	✓

Personal devices:

- The school accepts no liability for damage, theft or loss of any staff or student personal devices.

- The school does not offer technical support for personal devices.
- The school reserves the right to take, examine and search user's devices in the case of misuse.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully.
- Student's work can only be published with the permission of the student and / or parents.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Requirements (GDPR) which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

More information can be found in "Data Protection Privacy Notice Policies" for students and staff.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the academy	✓				✓			
Use of mobile phones in lessons			✓					✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras		✓						✓
Use of other mobile devices e.g. tablets,		✓					✓	

Use of personal email addresses in academy , or on academy network		✓					✓	
Use of academy email for personal emails				✓				✓
Use of messaging apps		✓						✓
Use of social media			✓					✓
Use of blogs			✓					✓

When using communication technologies the academy considers the following as good practice:

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Managing Email

Email is an essential means of communication for both staff and students. Directed email use can bring significant educational benefits; for example, projects between schools, locally, nationally and as part of the global community.

In the Academy context, email is not considered private and Henley-in-Arden Academy reserves the right to monitor academy email. However, there is a balance

to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, students and other professionals for any official academy business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

Students may only use approved email accounts for school purposes.

- Students must immediately tell a designated member of staff if they receive an offensive email.

- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.
- Spam, phishing and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

Emailing Personal, Sensitive, Confidential or Classified Information

- e-mailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted;
- Where the conclusion is that e-mail must be used to transmit such data it is essential that staff:
    - Obtain express consent from their line manager to provide the information by e-mail
    - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail
    - Verify the details, including accurate e-mail address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information;
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary. Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
    - Send the information as an encrypted document attached to an e-mail;

- Provide the encryption key or password by a separate contact with the recipient(s);
- Do not identify such information in the subject line of any e-mail;
- Request confirmation of safe receipt.

Managing Published Content

- The primary contact details on the website will be the academy address, email and telephone number. In order to make communicating with the academy as easy as possible we will also publish the email addresses of the senior leadership team (we reserve the right to remove these at any time).
- Other staff and all students' personal information should not be published.
- The Headteacher will take overall editorial responsibility for online content and ensure content is accurate and appropriate.
- The academy website will show respect for intellectual property rights, privacy policies and copyright.
- Photographs published on the website which includes students will be selected carefully and will comply with good practice guidance on the use of sexual images.
- Consent from parents or carers is obtained before photographs of students are published on the Academy website.

Social Media - Protecting Professional Identity

The academy has a duty of care to provide a safe learning environment for students and staff. We could be held responsible, indirectly for acts of our employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Academy staff should ensure that:

- Staff are expected to adhere to the appropriate sections relating to social networking in our Staff Code of Conduct.
- No reference should be made in social media (with the exception of school social media accounts such as the Twitter account) to students, parents or academy 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 academy
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The academy permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined process

The academy's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that any user should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					**X**
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					**X**
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					**X**
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					**X**
	Pornography				**X**	
	Promotion of any kind of discrimination				**X**	
	threatening behaviour, including promotion of physical violence or mental harm				**X**	
	Promotion of extremism or terrorism				**X**	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				**X**	
Using school systems to run a private business					**X**	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					**X**	
Infringing copyright					**X**	

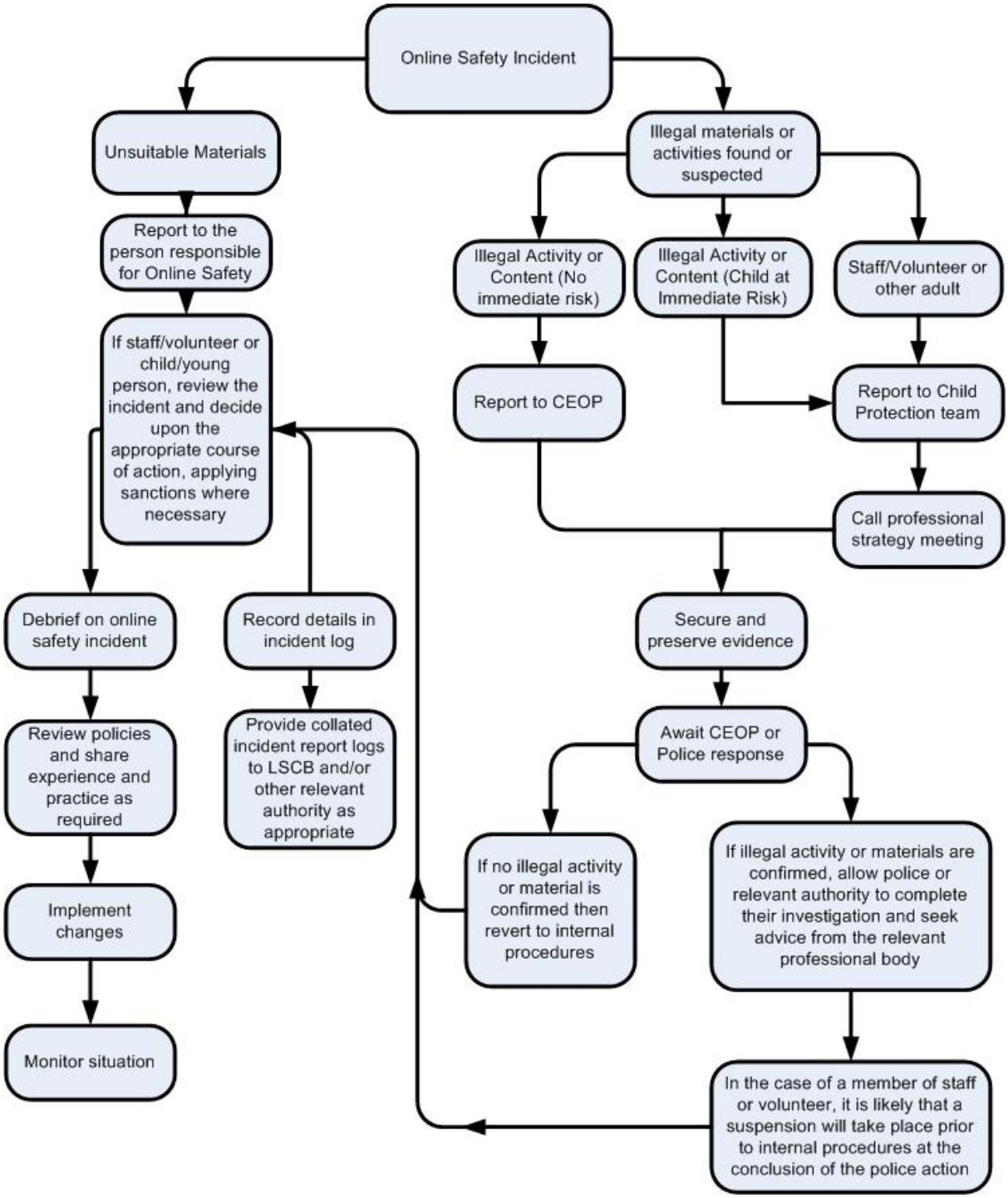
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce (staff only)			X		
File sharing	X				
Use of social media (staff only)			X		
Use of messaging apps (staff only)			X		
Use of video broadcasting e.g. YouTube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the green form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The resulting completed green form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary

procedures as per the school's behaviour policy (in the case of pupils) and the staff code of conduct and/or Staff Acceptable Use Agreement (in the case of staff).

Appendix A

Staff Acceptable Use Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users. Please ensure you understand your responsibilities under this policy and direct any questions or concerns to the IT Network Manager in the first instance.

All members of staff have a responsibility to use the Henley-in-Arden school computer system in a professional, lawful and ethical manor. Please respect these guidelines many of which are in place for your protection. Deliberate abuse of the Academy computer system may result in disciplinary action (including possible termination) and civil and/or criminal liability.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the school digital technology and communications systems including my email account and storage areas provided for my use to ensure compliance with this acceptable user agreement, and applicable laws. This may include remote monitoring of devices. In particular the academy computers a complete record of sites visited on the internet by both students and staff (however usernames and passwords used on those sites are not monitored or recorded).
- I will avoid storing sensitive personal information on the Academy computer system that is unrelated to Academy activities (such as personal passwords, photos or financial information).
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will not allow a student to have individual use of my staff account under any circumstances, for any length of time, even if supervised.
- Pupils must be supervised at all times when using academy computer equipment. When arranging use of computer facilities I will ensure supervision is available.
- I will ensure the separate acceptable use agreement for pupils is enforced when I am supervising pupils using school computer equipment.

- When leaving a computer unattended, I will ensure I have either logged off my account or locked the computer to prevent anyone using my account in my absence.
- If I use a personal device for work purposes I will ensure that any Henley-in-Arden School related sensitive or personal information is secured to prohibit access by any non-member of staff and encrypted to protect against theft.
- I will ensure that portable computer equipment (such as laptops, iPads, Mobile Phones, Digital Cameras etc.) are securely stored in a locked room or cupboard when unattended.
- Equipment taken offsite is not routinely insured by the academy. If I take any School equipment offsite, I will ensure that adequate insurance cover has been arranged to cover against loss, damage or theft.
- I will immediately report any illegal, inappropriate or harmful material, incident (including bullying or harassment) or breaches / attempted breaches of security, I become aware of, to the IT Network Manager or Headteacher. All reports will be treated confidentially.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- When using my school email address for communication both internally and both other email users outside of the academy, I understand that email has the same permanence and legal status as written hardcopy (paper) documents and maybe subject to disclosure obligations in exactly the same way.
- I understand email to outside organisations has the same power to create a binding contract as hardcopy documents. I will not purchase goods or services on behalf of the academy via email without proper authorisation.
- I agree that all Academy email I sent will have a signature containing my name, job title and the name of Henley-in-Arden Academy.
- I understand email is not a secure method of communication and as such I will not transmit or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the Academy.
- I understand the academy will take measures to minimise the receipt and impact of unsolicited email containing offensive and/or sexually explicit content but that it cannot held responsible for material received or reviewed by me from the internet.
- I will not send chain letters or unsolicited commercial email (also known as spam).
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal

information, those who are featured (unless parental consent has been obtained).

- I will only use social networking sites in school in accordance with the school's policies. In particular:
  - I will not allow any pupil access to personal information I post on a social networking site.
  - I will not add a pupil to my friends list
  - I will avoid contacting any pupil privately via social networking website, even for Henley in Arden School purposes.
  - I will take steps to ensure that any person contacting me via a social networking website are who the claim to be, and not an imposter, before allowing them to access my personal information.
  - I will not post content on websites which appear as I am speaking for the academy, unless I have been authorised to do so.
  - I must not post material online which can be clearly linked to the academy which may damage Henley-in-Arden schools reputation.
  - I will avoid posting any material clearly identifying myself, another member of staff or a student that could potentially be used to embarrass, harass or defame the subject.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will make my own backup of data kept on any storage system other than the designated network storage drives. This includes USB memory sticks (even those owned or issued by the academy) or a personal device.
- I will not try to upload, download access or transmit any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate (vulgar, suggestive, obscene, abusive, harassing, threatening, sexist or defamatory) or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will try to not intentionally waste resources. Examples of such wastage include:
  - Making large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
  - Excessive storage of unnecessary files on the network.

    - Excessive use of colour printing or not collecting/using printing from the printers.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- Where an iPad has been issued to me, I will not change the security settings and will not synchronised with my personal settings, photos, videos etc.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy e-Safety / Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will report any other computer system problems or faults that need attention to a member of IT Support Staff as soon as is feasible. Problems that seriously hinder my job or teaching I will report immediately by telephone; any other problems I will report via the online helpdesk.
- If I suspect that my computer has been affected by a virus or other malware, I will report this to a member of the IT Network Manager immediately.
- If I have lost documents or files I will report this as soon as possible to the IT Support Staff (the longer a data loss problem goes unreported the lesser the chances of the data being recoverable).
- I will avoid eating or drinking around computer equipment.

When using the internet or academy computer systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will consult the IT Network Manager before placing any order for computer hardware or software, or obtaining and using any software I believe to be free. This is to check that the intended use by the academy is permitted under copyright law (as well as to check compatibility and discuss other implications that the purchase or download may have).
- By storing or creating any personal documents or files on the academy computer system I grant the Academy a non-exclusive, universal, perpetual, irrevocable and royalty-free licence to use, copy and distribute those documents or file is any way the Academy sees fit.

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy.
- I understand that occasional personal use of the schools computers and IT systems:
    - Must not interfere with my other duties or those of other members of staff
    - Must not have any undue effect on the performance of the computer system
    - Must not be for any commercial purpose of gain unless explicitly authorised by the Headteacher.

  Personal use is permitted at the discretion of Henley-in-Arden school and can be limited or revoked at any time.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors in the event of illegal activities the involvement of the police.

This Acceptable Use Agreement will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example; significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to the policy will be communicated to all staff. Due to the fast paced nature of technological change, and the important safeguarding nature of this agreement we will require all staff to demonstrate their knowledge and acceptance of this end user agreement.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name ……..

Staff / Volunteer Signature …….

Date ……

Appendix B

Responsible Use of ICT by Students

Computer Safety

- Use of social networking sites is not allowed in school.

- I will tell a teacher immediately about any unpleasant, inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it. These reports will help protect others as well as myself.
- I must not give personal details, home addressed or telephone numbers or arrange to meet anyone via the Internet.
- I understand that Henley-in-Arden School can remotely monitor what I do on the school computers. The school maintains the right to check the use of all computers and devices used in school at any time.
- I understand that the school web content is filtered and is there to protect me and the computer network. I will not try to bypass this filter. If I need access to a blocked website I will ask my teacher.

Computer Care

- I will not install or download any software or programs onto school equipment. If I require a new program, I will ask a teacher for this – I will not try to install this myself.
- I will not try to connect any personal devices to the school network, without direct permission.
- I will only change settings on the computer if I'm allowed to do so.
- I know that food and drink is not allowed in computer rooms under any circumstances.
- I understand that deliberate damage to the computer equipment and any unauthorised access to files, is not allowed and may be considered a criminal offence under the Computer Misuse Act 1990.
- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed. I won't leave it broken for the next person.
- I understand that loan laptops and tablet device are property of Henley-in-Arden School. I will treat them with care and respect and will return them, on time and in the condition that they were supplied.

Personal Responsibility

- I understand that access to the school network must only be made via my authorised school username and password, which must not be given to any other person.
- All emails I write should be written carefully and politely.
- I understand that school internet access is a privilege, not a right. It will be taken away from me if I abuse it.
- I understand that installing, viewing, copying or transmitting of obscene material is forbidden and may be considered a criminal offence under the Criminal Justice & Public Order Act 1984.
- Unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act, is not permitted.
- School computer and Internet use must be appropriate to the student's education.
- I will only upload pictures and videos from inside Henley-in-Arden School, or taken during school time, if I have permission.
- I will not take or distribute pictures or videos of any without their permissions.
- I will only download music or videos onto the computer if it is related to my school work.

- I will always treat other the same way I would want them to treat me. I will not use the computers to harass or bully anyone.
- I will be polite online, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.

Sanctions:

1. If rules are breached, use of school network may be restricted or withdrawn.
2. Further disciplinary action may be taken in line with the School Behaviour Policy.
3. In severe cases, police or other authorities may be involved.

As a School user of the internet, I agree to comply with the Rules of Use.

Student Name …….. **Form ……**

Student Signature ……

As the parent or legal guardian of the above student, I give my permission for my son or daughter to hold an Internet and email account at Henley in Arden School in accordance with the rules outlined above.

Signature of Parent or Guardian ……. **Date ……**

Appendix C

Responsible Internet Use – Rules

The computer system is owned by the school and as such is open to being monitored at all times. These rules are to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- **Network access MUST be made via the user's authorised account and password – which MUST NOT be given to any other person.**
- **School computer and internet use is only for student education or staff professional activity.**
- **Users are responsible for email they send and for contacts made**
- **Emails should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.**
- **Anonymous messages and chain letters are NOT permitted**
- **The use of chatrooms is NOT allowed**
- **Copyright and intellectual property rights MUST be respected.**
- **The school IT systems must not be used for private purposes unless the Headteacher has provided permission for that use**
- **Use for personal financial gain, gambling, political purposes or advertising is NOT permitted.**
- **ICT system security MUST be respected: it is a criminal offence to use a computer for a purpose not permitted by the system owner.**
- **Any damage to IT equipment MUST be reported immediately**
- **You MUST immediately inform a member of the IT Network staff, or the Principal, of any abuse, misuse or access to inappropriate materials on any part of the school computer system.**
- **Irresponsible use may result in the loss of internet access and more serious breaches may be open to further sanctions or reported to the appropriate authorities**

Appendix D

Legal Framework

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. Specific legislation pertaining to e-safety includes the following:

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

The School Information Regulations 2012
Requires schools to publish certain information on its website:

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour / anti bullying policy.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Head Teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

It is recommended that legal advice is sought in the advent of an e safety issue or situation.