Hednesford Valley High

E-Safety / Cyber Security Policy

Reviewed by:	D Watson
Last reviewed:	September 2025
Next review due by:	July 2027

Website: www.hvh.staffs.sch.uk **Headteacher**: Mr S. Stokes, BSc (Hons), PGCE, NASENCo
Assistant Headteachers: Mrs E Hill, BSc (Hons), QTS, NPQSL, MA, Mrs E Perry, BSc (Hons), PGCE, PGDip,MA,NASENCo
Associate Assistant Headteacher: Mr C Wall, BSc (Hons), PGCE, NPQML

Change log

January 2024:

[added lines] (staff are responsible for ensuring)

- are familiar with use of the school's safety and/or safeguarding software
- are actively monitoring student's IT usage in their classroom
- they act immediately if they have any concerns about a child's welfare
- they follow DfE and KCSiE guidance on issuing disciplinary action (in accordance with the schools behaviour policy) against students who breach Acceptable Use policies or rules on social media use, inside or outside of school.

Section 4 [change line] (The school will therefore seek to provide information and awareness to Parents/Carers through:)

- Letters, newsletters, online services/presence (including school website **and social media**)

Section 8 [added line] Staff should not transfer restricted or confidential data to personal cloud storage without authorisation from their IT department.

September 2025

Section 2 [changed line] (governors…will meet with eSafety co-ordinator)

- regular meetings with the IT Manager and Safeguarding Team (or person responsible for eSafety)
- clarified role of eSafety Lead, removing esafety committee references and including updating governors. SLT and the safeguarding team.

[changed Headteacher]

- day to day responsibility for e-safety will be delegated to a person responsible for leading eSafety, who will also be on the safeguarding team.

[added] teaching and support staff are to [be aware of esafety legislation and risks].….

- This includes the four key categories of risk: content, contact, conduct and commerce; as well as their definitions.
- Ensure products containing artificial intelligence are tested prior to use and if used by pupils are secured robustly against exposure to harm or prohibited material. This may also involve carrying out a risk assessment prior to use.
- Ensure any content generate by artificial intelligence is accurate, does not contravene copyright or intellectual property laws and is not stored or copyrighted by the company/product before being put into live usage (such as in resources or school website etc)

Section 3 [added]

- *Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies*

Section 8 [added]

- [Staff should] Ensure products build around, or containing, Artificial Intelligence should be secured against malicious use. Particularly if personal data is uploaded to a third party. In this instance DPO should be informed and IT staff tested the product before use to ensure the product is data protection compliant and not based in a country that could put data integrity at risk. DPIA forms should be completed. **All AI generated content should be checked for accuracy before used in a live environment or published**.

1. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, and within the boundaries of legal, privacy and child protection policies/procedures, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti -bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Cyber Security should also be considered as part of safety, along with other IT policies to ensure a safety net for users and their data.

2. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Board has taken on the role of E-Safety, the role of the E-Safety Governor will include:

- regular meetings with the IT Manager and Safeguarding Team (or person responsible for eSafety)
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meetings

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety and cybersecurity) of members of the school community, though the day to day responsibility for e-safety will be delegated to a person responsible for leading eSafety, who will also be on the safeguarding team.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their e-safety/cyber security roles and to train other colleagues, as relevant.
- Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

- The Senior Leadership Team will review IT services that store personal data, or require substantial changes to IT systems, to ensure the data being transferred to third parties is required and that appropriate security protects this data.

E-Safety Lead/Safeguarding Team:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team and Safeguarding Team

Network Manager:

The Network Manager/Co-ordinator for Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack that the school meets required e-safety/cyber security and technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- that users where technically possible may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network/internet/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher, Senior Leader; E-Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies
- that users have 'just enough' administrative access that their role requires
- that third party services are audited for data security and to ensure DPO/SLT are aware of any potential safeguarding or data security issues before staff are given access.

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of e-safety/(relevant) cyber security matters and of the current *school* e-safety policy and safe practices. This includes the four key categories of risk: content, contact, conduct and commerce; as well as their definitions.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Headteacher, Senior Leader, E-Safety Lead* for investigation/action/sanction
- they follow the guidance and IT procedures given by senior staff
- they take steps to ensure that data is secure and that new software or cloud services are trialled before purchase to ensure the security of the data
- are familiar with use of the school's safety and/or safeguarding software

- are actively monitoring student's IT usage in their classroom
- they act immediately if they have any concerns about a child's welfare
- they follow DfE and KCSiE guidance on issuing disciplinary action (in accordance with the schools behaviour policy) against students who breach Acceptable Use policies or rules on social media use, inside or outside of school.
- Ensure products containing artificial intelligence are tested prior to use and if used by pupils are secured robustly against exposure to harm or prohibited material. This may also involve carrying out a risk assessment prior to use.
- Ensure any content generate by artificial intelligence is accurate, does not contravene copyright or intellectual property laws and is not stored or copyrighted by the company/product before being put into live usage (such as in resources or school website etc)

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use 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 cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying. should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

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 school will take every opportunity to help parents/carers understand these issues through Parents' evenings, newsletters, letters, website/VLE and information about national/local e-safety campaigns/literature. Parents/Carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to Parents' sections of the website/VLE and on-line student records
- their children's personal devices in the school/academy (where this is allowed)

3. Securing Equipment, Networks and Data – All Users

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. (KCSIE 2025)

All users of equipment, networks, cloud services and those with access to data must adhere to the following rules:

- Only use your own usernames and passwords and never share their login information with others.
- Use complex passwords that cannot easily be guessed.
- Do not write down your password.
- Use Multi Factor (2 Factor) Authentication (2FA/MFA) at all times, where available.
- For clarity: key cards, fobs or other tools (such as smart watches) can be used to aid securing or unlocking devices – but must also be secured where possible
- Ensure your account recovery information is kept up to date.

- Do not attempt to access areas that you are not authorised to access.
- Lock your screen when away from your device.
- Encrypt all data, or store data in an authorised password protected cloud, that is removed from the site (as detailed in section 7).
- Ensure any non-school devices are password protected and have a working internet security software package installed and correctly configured before school data or networks are accessed (as detailed in section 5).
- Do not remove any security software, policies or profiles from any device (as detailed in section 2 of the Acceptable User Policy)
- Ensure all new or previously unused equipment or cloud services holding data are secure by testing and trialling before orders are placed and before transferring any data to them.
- Follow all guidance, procedures and policies for IT usage as set out in policy, training or communications (emails/bulletins/staff meetings etc)

4. 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key e-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 helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school
- Staff 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, 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.

Education – Parents/Carers :
Many parents/carers have only a limited understanding of e-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/Carers 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 school will therefore seek to provide information and awareness to Parents/Carers through:

- Curriculum activities
- Letters, newsletters, online services/presence (including school website and social media)
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community:
The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards Grandparents and other relatives as well as parents/carers.
- The school website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Child-minders, youth/sports/voluntary groups to enhance their e-safety provision

Education & Training – Staff/Volunteers:
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Lead/Network Manager receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations. (in e-safety and cyber security)
- This E-Safety policy and its updates will be presented to and discussed by staff in Staff /team meetings/INSET days.
- The E-Safety Lead/Network Manager will provide advice/guidance/training to individuals as required.

5. Training - Governors

Governors should take part in e-safety and cyber security training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (eg SWGfL).
- Participation in school training/information sessions for staff or parents/carers (this may include attendance at assemblies/lessons).

- School technical systems will be managed in ways that ensure that the school meets recommended technical
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password 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 and will be required to change their password every 60 days.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)

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 (i.e 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. There is a clear process in place to deal with requests for filtering changes.

- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc.)
- School staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6. Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training,

support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
  Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy
- BOYD devices are all protected with internet security software.

7. 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in 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 image.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes without express written consent of SLT.
- 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 school 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 and will comply with good practice guidance on the use of such images.
- Students photos or likenesses should not be uploaded to any cloud service until security has been assessed. For clarity this includes profile pictures.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUA signed by parents/carers at the start of the year - see Parents/Carers Acceptable Use Policy in the appendix)
- Student's work can only be published with the permission of the student and parents/carers.

8. Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR regulations 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.
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a GDPR Policy. It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out. It has clear and understood arrangements for the security, storage and transfer of personal data.
- Thirds party services used to store data are fully trialled and tested before purchased and data is transferred.
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Where possible, minimise the use of USB Pen Drives or external drives.
- Ensure products build around, or containing, Artificial Intelligence should be secured against malicious use. Particularly if personal data is uploaded to a third party. In this instance DPO should be informed and IT staff tested the product before use to ensure the product is data protection compliant and not based in a country that could put data integrity at risk. DPIA forms should be completed. **All AI generated content should be checked for accuracy before used in a live environment or published.**

When any school or personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

When any third party service, such as a cloud service, is used to store personal or school data:

- A full trial must be carried out before any purchase in order to assess suitability and security
- The IT department must clear a service for use before any personal data is transferred to it
- Only staff whose role requires full administrative access should have it. All other should have 'just enough' rights delegated for them to be able to carry out their duties.

Any data breach or leak must be reported as soon as possible and all reasonable attempts made to rectify the leak (email recall, closing down the PC etc)

Staff should not transfer restricted or confidential data to personal cloud storage without authorisation from their IT department.

When using communication technologies, the school considers the following as good practice:

- The official school email service and separate communication/texting service is regarded as safe and secure as long as restricted/confidential emails are marked and encrypted and the system is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school 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, chat, online posts.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-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.

9. Social Media – Protecting Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of

harm to students, staff and the school through limiting access to personal information:

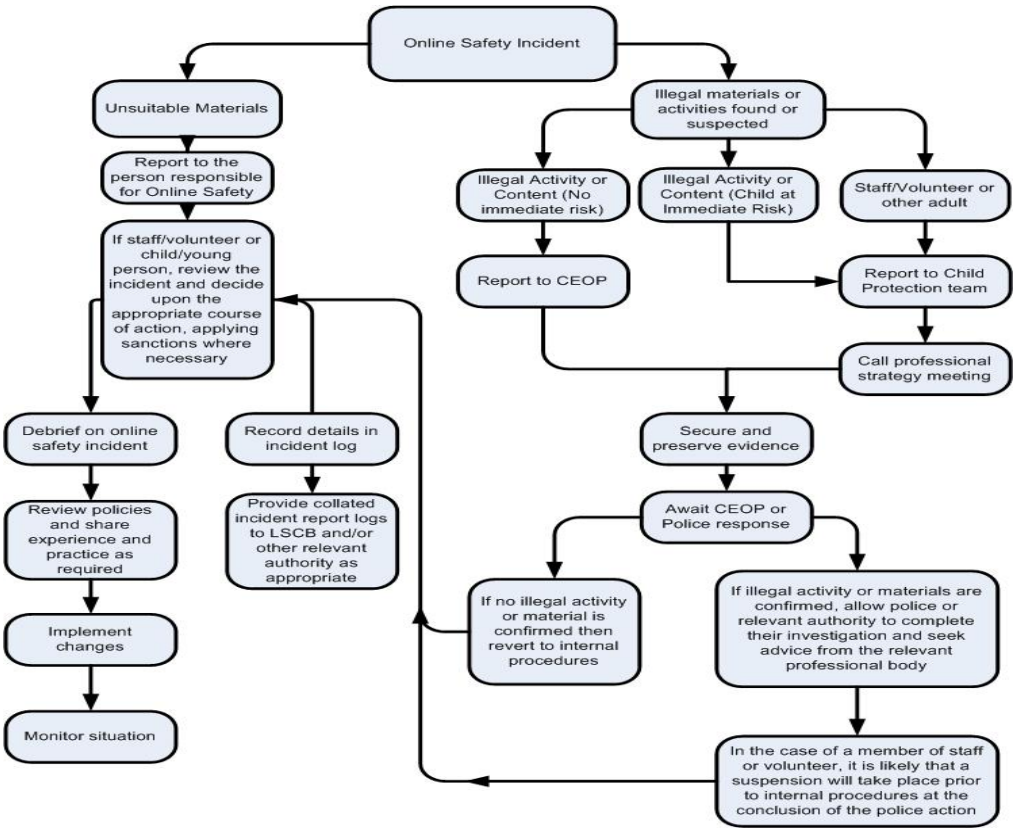
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- School staff should ensure that:
- No reference should be made in 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* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

10. 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.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who

understand and follow school 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 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
- Involvement by Local Authority or national/local organisation (as relevant).
- 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
- other criminal conduct, activity or materials

Isolate the computer or user account 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 school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

Users Accounts/Services may be limited or suspended while investigations are carried out. Or access to features removed if a user is suspected of failing to comply with a reasonable policy or procedure in order to protect the account, other users or the integrity of any investigation – formal or informal.
It is more likely that the school 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.

11. Rules and Sanctions for Students

Students will be aware that they need to adhere to the acceptable use policy. In order to use the school's network, the students will click to say they accept the agreement.

If students are found to not be adhering to the acceptable use policy the following sanctions will take place, on the first occasion students will receive a warning, if students are found to be not adhering to the acceptable use policy on more than one occasion students will then receive limited internet access for a period of a day. In more serious misuse cases students will receive a full Internet ban and parents/carers will be notified by letter. Sanctions are determined in line with the school behaviour policy.

12. Repeat Offenses / Serious Concerns

Students will be aware that they need to adhere to the acceptable use policy which will be updated from March 2019. In order to use the school's network the students will click to say they accept the agreement.

If students are found to not be adhering to the acceptable use policy the following sanctions will take place, on the first occasion students will receive a warning, if students are found to be not adhering to the acceptable use policy on more than one occasion students will then receive limited internet access for a period of a day. In more serious misuse cases students will receive a full Internet ban and parents/carers will be notified by letter.

Students who commit multiple misuse offenses will have tailored consequences including, but not limited to, extended internet bans, full technology bans (to be determined on a case-by-case basis) and referral to the main school behaviour policy (where relevant, such as cases of bullying, swearing, intimidation, poor work rate in lessons, cheating in coursework, damage to property in relation to a physical outburst caused by use of or removal of technology).

More serious offenses, or multiple offenses that when assessed collectively cause concern about the welfare of a student or others, shall be recorded on MyConcern for the safeguarding team to assess whether further help is required. In this instance the student shall be placed on a Digital Support Plan (DSP). These are similar to Risk Assessments but confined to usage of digital equipment. Staff will treat DSPs in the same way as a risk assessment and ensure they are carried out for as long as the dates (if declared) state.

Digital Support Plans are used when a student, or others, could be put at risk by being allowed use of any technology without careful supervision; but continually denying access (such as described in 12a) could have a negative impact on their education. These plans will declare the risks and describe the control methods, such as supervision requirements while using technology, who is responsible for actioning the control methods and, if required, a review date.

Staff will ensure that all the control methods are strictly adhered to, similar to a risk assessment, for the safety of the student.

The student will not normally be granted permission to use any technology unless the plan specifically specifies it. The student will be denied the right to bring any technology into school, unless requested by parents/carers. In this instance, the technology will be surrendered upon entry and locked away until the student leaves at the end of the school day.

See Digital Support Plan template in Appendix 1.

13. Dissemination and Review

The policy will be disseminated widely both to Staff and Governors through appropriate meetings.

The policy will be reviewed October 2024.

Appendix 1: Digital Support Plan form

HVH DIGITAL SUPPORT PLAN		
Name: Date	ACTIVITY / EQUIPMENT: N/A	
People involved in writing this plan:		
HAZARDS	CONTROL MEASURES	FURTHER ACTION REQUIRED

This is to be reviewed –1.5.18

DRAFT