HACKBERRY

ALTERNATIVE PROVISION

ONLINE SAFETY POLICY

Policy publication date	02/09/2025
Policy agreed by	S Trevethan / R Childs
Policy review date	02/09/2026

Contents

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by Hackberry

- Directors
- Staff – including Teachers, Support Staff, Technical staff
- Parents and Carers
- Community users

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors	8/7/2025
The implementation of this Online Safety policy will be monitored by the:	Directors
Monitoring will take place at regular intervals:	2/9/2025
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	2/9/2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Safeguarding Office, Student's School and/or police

Hackberry will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

Scope of the Policy

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

The Education and Inspections Act 2006 empowers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off Hackberry site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other Online Safety incidents covered by this policy, which may take place outside of Hackberry, but is linked to membership of Hackberry. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Hackberry will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform the students/pupils school, parents / carers of incidents of inappropriate Online Safety behaviour that take place out of Hackberry.

Roles and Responsibilities

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

Board of Directors

Directors 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 Directors receiving regular information about online safety incidents and monitoring reports. A member of the Board has taken on the role of Online Safety Director The role of the Online Safety Director will include:

- regular meetings with the Online Safety Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Board

Senior Leaders

- The Director has a duty of care for ensuring the safety (including online safety) of members of Hackberry community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Officer / Lead.
- The Director and (at least) another member of the Senior Management Team 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 – included in a later section – “Responding to incidents of misuse” and relevant Local Authority / MAT / other relevant body disciplinary procedures).
- Staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Directors will ensure that there is a system in place to allow for monitoring and support of those in Hackberry who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Directors will receive regular monitoring reports.

Online Safety Officer / Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing Hackberry 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 Hackberry technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- students will not have access to the internet at Hackberry
- Principal / Senior Leader; Online Safety Officer / Lead for investigation / action / sanction that monitoring software / systems are implemented and updated as agreed in Hackberry policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Hackberry Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Officer for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils 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 activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils 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

Designated Safeguarding Lead / Designated Person / Officer

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision

Students / Pupils:

- 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of Hackberry and realise that Hackberry's Online Safety Policy covers their actions out of Hackberry, if related to their membership of Hackberry.

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. Hackberry will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support Hackberry in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at events
- their children's personal devices in Hackberry (where this is allowed)

Policy Statements

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students /

pupils in online safety / digital literacy is therefore an essential part of the Hackberry's online safety provision. Children and young people need the help and support of Hackberry 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.
- Students / pupils 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 / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils 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. N.b. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Hackberry.
- 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 / pupils 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 / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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 online 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.

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

- Website

Education – The Wider Community

Hackberry will provide opportunities for local community groups / members of the community to gain from Hackberry online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- Hackberry website will provide online safety information for the wider community

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:

A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly

All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Hackberry Online Safety Policy and Acceptable Use Agreements.

It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Officer / Lead (or other nominated person) will provide advice / guidance / training to individuals as required

Training – Governors / Directors

Directors should take part in online safety training / awareness sessions, this may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.

Technical – infrastructure / equipment, filtering and monitoring

Hackberry will be responsible for ensuring that the 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:

Hackberry technical systems will be managed in ways that ensure that the Hackberry meets recommended technical requirements There will be regular reviews and audits of the safety and security of Hackberry technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Hackberry technical systems and devices.
- Users are responsible for the security of their username and password and will be required to change their password every 8 weeks.
- The “master / administrator” passwords for Hackberry ICT systems, used by the Network Manager (or other person) must also be available to the Director or other nominated senior leader and kept in a secure place (e.g Hackberry safe)
- Director 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. 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.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Hackberry technical staff regularly monitor and record the activity of users on the technical systems and users are made aware of this in the Acceptable Use Agreement.
- 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 systems and data. These are tested regularly. The infrastructure and individual workstations are protected by up-to-date virus software.
- There will be no temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place, no staff other than Directors are allowed on devices that may be used out of Hackberry.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on Hackberry 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 site unless safely encrypted or otherwise secured.
- Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile / personal devices in a Hackberrycontext is educational. The mobile technologies policy should be consistent with and inter-related to other relevant policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Online Safety education programme.

- Hackberry's Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	Hackberry Devices			Personal Devices		
	Hackberry owned for single user	Hackberry owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in Hackberry	Yes	Yes	Yes	No	No	No
Full network access	Yes	Yes	Yes	N/A	N/A	N/A
Internet only	Yes	No	Yes			
No network access				Yes	Yes	Yes

Aspects that Hackberry may wish to consider and be included in their Online Safety Policy, Mobile Technologies Policy or Acceptable Use Agreements:

Hackberry owned / provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times / places / in Hackberry / out of Hackberry
- If personal use is allowed
- Levels of access to networks / internet (as above)
- Management of devices / installation of apps / changing of settings / monitoring

- Network / broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking / storage / use of images
- Exit processes – what happens to devices / software / apps / stored data if user leaves Hackberry
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in Hackberry (staff / pupils / students / visitors)
- Restrictions on where, when and how they may be used in Hackberry
- Storage
- Whether staff will be allowed to use personal devices for Hackberry business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users' devices in the case of misuse (England only)
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network
- Identification / labelling of personal devices
- How visitors will be informed about Hackberry requirements
- How education about the safe and responsible use of mobile devices is included in the Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils 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.

When using digital images, staff should inform and educate students / pupils 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 / pupils are published on the Hackberry 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 Hackberry 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 / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow Hackberry policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Hackberry equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or Hackberry into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Hackberry must ensure that:

- It has a privacy notice.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).

- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- Hackberry has a privacy notice which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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.

When 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 device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with Hackberry policy once it has been transferred or its use is complete.

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 & other adults			Students / Pupils				
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 Hackberry								
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, gaming devices								
Use of personal email addresses in Hackberry, or on Hackberry network								
Use of Hackberry email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

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

- The official Hackberry email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the Hackberry email service to communicate with others when in school, or on Hackberry systems (e.g. by remote access).

- Users must immediately report to the nominated person – in accordance with the Hackberry 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 / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Hackberry systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils school will teach 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 by student / pupil school and Hackberry.
- Personal information should not be posted on the Hackberry website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the Hackberry liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Hackberry provides the following measures to ensure reasonable steps are taken to minimise risk of harm to pupils, staff and Hackberry 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

Hackberry staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or Hackberry 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 Hackberry
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official Hackberry social media accounts are established there should be:

- A process for approval by senior leaders

- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under Hackberry disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with Hackberry or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of Hackberry 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 Hackberry is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

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
- Hackberry should effectively respond to social media comments made by others according to a defined policy or process

Hackberry's use of social media for professional purposes will be checked regularly to ensure compliance with Hackberry policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Hackberry 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 Hackberry, either because of the age of the users or the nature of those activities.

Hackberry believes that the activities referred to in the following section would be inappropriate in a Hackberry context and that users, as defined below, should not engage in these activities in / or outside of Hackberry when using Hackberry equipment or systems. The Hackberry policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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 Hackberry systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Hackberry					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	

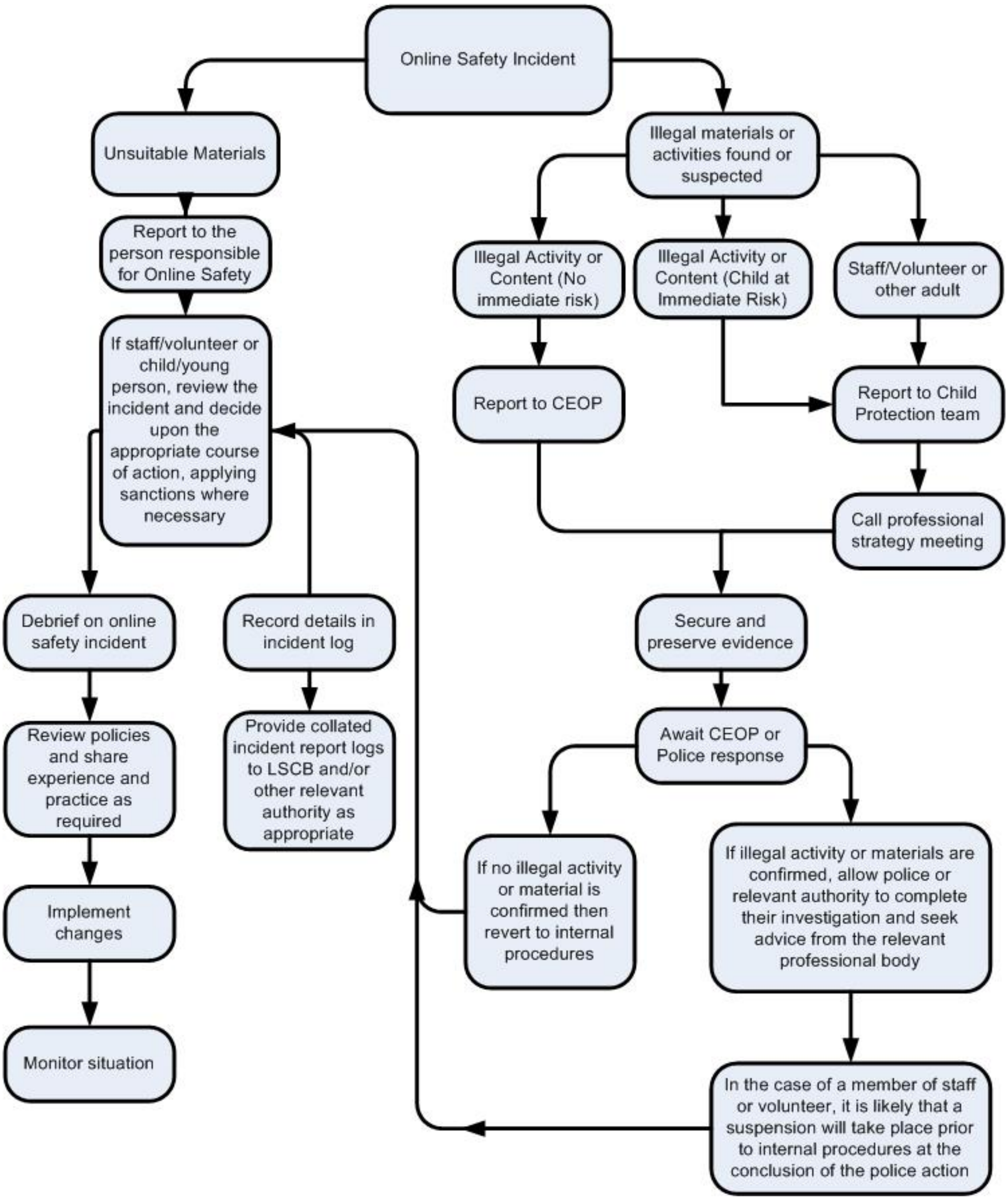
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping / commerce					
File sharing					
Use of social media					
Use of messaging apps					
Use of video broadcasting e.g. Youtube					

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 and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the Hackberry community will be responsible users of digital technologies, who understand and follow Hackberry 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 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 / Academy Group 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
    - 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 Hackberry and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Hackberry Actions & Sanctions

It is more likely that Hackberry 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 follows:

Students / Pupils Incidents		Refer to Director	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers and school	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X					
Unauthorised use of non-educational sites during lessons		N/ A					
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X		X			
Unauthorised / inappropriate use of social media / messaging apps / personal email		X		X			
Unauthorised downloading or uploading of files		X		X			
Allowing others to access Hackberry network by sharing username and passwords		N/ A					
Attempting to access or accessing the Hackberry		N/					

network, using another student’s / pupil’s account		A					
Attempting to access or accessing the Hackberry network, using the account of a member of staff		X		X			
Corrupting or destroying the data of other users		X		X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X			X
Actions which could bring Hackberry into disrepute or breach the integrity of the ethos of the school		X		X			X
Using proxy sites or other means to subvert the Hackberry filtering system		X		X			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X			
Deliberately accessing or trying to access offensive or pornographic material		X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X			X

Staff Incidents	Refer to line manager	Refer to Director	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X				X
Inappropriate personal use of the internet / social media / personal email	X	X			X		
Unauthorised downloading or uploading of files	X	X			X		
Allowing others to access Hackberry network by sharing username and passwords or attempting to access or accessing the Hackberry network, using another person's account	X	X			X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X		
Deliberate actions to breach data protection or network security rules	X	X			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X			X	X	X

Actions which could compromise the staff member’s professional standing	X	X					X
Actions which could bring Hackberry into disrepute or breach the integrity of the ethos of the Hackberry	X	X			X	X	X
Using proxy sites or other means to subvert the Hackberry filtering system	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X	X
Breaching copyright or licensing regulations	X	X					
Continued infringements of the above, following previous warnings or sanctions		X					X