ghes
educating with confidence
GLOUCESTERSHIRE HOSPITAL EDUCATION SERVICE

Gloucestershire
COUNTY COUNCIL

Policy Name: Online Safety & Acceptable Use of ICT	
Last updated:	October 2025
Date of next review:	September 2026 (to bring into line with KCSIE 2026 updates)
Member of staff responsible for the policy:	Beth Warren
Dissemination of the policy:	Management Committee, staff, website

CONTENTS

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of

- Head of Service
- Online Safety Group
- Learning Technologist
- Staff – teaching and support staff
- Members of the Management Committee
- Parents

Scope of the Policy

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within GHES.

The policy has been written predominantly for the Outreach side of the service. We acknowledge that for the students and staff on GRH Children's Ward, many aspects of this policy especially in regard to the teaching and learning, and support for parents will be more limited due to the nature of the ward setting.

Management Committee (MC)

The Management Committee is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. The direct link with the MC is the Chair. The role includes:

- Monitoring visit with Online Safety Lead
- Reporting to relevant Management Committee meetings
- Ensuring online safety is considered when reviewing any ICT software or applications.

Head of Service

The Head of Service has a duty of care for ensuring:

- The safety of members of the school community, though the day to day responsibility for online safety is delegated to the learning technologist and safeguarding team of staff.
- Another member of the Senior Leadership Team is also aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. *Ref: GHES Allegations Management Procedure.*
- That all staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Where the training includes:

    - How to identify online risks
    - How to respond to online safety concerns
    - Understanding the filtering and monitoring systems in place

Designated Safeguarding Lead (DSL)

- Takes day to day 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.
- Monitoring and reporting on online safety issues to the Senior Leadership team (SLT), (MC) and other agencies as appropriate.
- Acting as a named point of contact for online safety issues.
- Liaises with the Local Authority.
- Ensure staff are aware of SEND-specific online risks and how to support vulnerable learners

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

Content Risks
Exposure to misinformation, disinformation, and conspiracy theories
Harmful or inappropriate online material (e.g. violence, hate speech, pornography)
AI-generated content that may be biased, misleading, or inappropriate

Contact Risks
Online grooming or exploitation by strangers
Inappropriate contact via social media, gaming platforms, or messaging apps
Radicalisation or recruitment by extremist groups

Conduct Risks
Cyberbullying and peer-on-peer abuse
Sharing of inappropriate images or messages (e.g. sexting)
Risky or harmful online behaviour (e.g. trolling, oversharing)

Commerce Risks
Exposure to scams, fraud, and exploitative advertising
In-app purchases or online spending without understanding risks
Data harvesting or misuse of personal information

Emerging Technology Risks
Unsafe or unethical use of generative AI tools
Lack of understanding of how AI works and its limitations
Data protection breaches through AI or digital platforms

Systemic Risks
Inadequate filtering and monitoring systems in schools
Lack of staff training on new and evolving online threats

Insufficient pupil education on digital resilience and critical thinking

Online Safety Group

- To discuss new or developing issues, e.g., new apps children/young people are using, new games, emerging risks etc.
- To review the online safety policy annually or in response to an incident.
- To annually monitor the online safety incident log and any concerns raised.
- To discuss training needs of all staff, and parent awareness.
- To raise new initiatives in response to training needs or as a result of polls/surveys.
- To review the online safety curriculum with other relevant members of staff, e.g., PSHE lead, ensuring that it is tailored to fit the needs of all students and statutory requirements.
- Ensure that online safety is promoted to parents and carers and the wider community through various mechanisms, such as the parent bulletin, parent newsletters and through other ad hoc events
- Provides resources and materials for staff to use in lessons, and for Link Tutors to use in their sessions, as well as taking part in national events such as Safer Internet Day.

Learning Technologist

The Learning Technologist is responsible for ensuring:

- That the GHES Curriculum infrastructure is appropriate for the setting and meets DfE standards for a school. *Ref: Online Safety Audit*
- That GHES meets required online safety technical requirements and any GCC online safety policy/guidance that may apply. *Ref: Online Safety Audit*
- That users may only access the GHES Curriculum network and devices through a properly enforced password *Ref: GHES ICT Technical Policy*
- The filtering section of the ICT Technical Policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. *Ref: GHES ICT Technical Policy*
- 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 GHES curriculum network at GHES outpatients is regularly monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies. *Ref: Online Safety Audit*
- To ensure that age-appropriate filtering is in place, which is actively monitored
- Reviewing and updating e-Safety policies, Acceptable Use Policies and other procedures on a regular basis (at least annually) with the Designated Safeguarding Lead.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current GCC and GHES online safety policy and practices.
- They have read, understood and signed the GCC staff acceptable use policy [this is part of the new staff induction process, and updates to all staff as appropriate].
- They report any suspected misuse or problem to the Head of Service for investigation.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in the PSHE curriculum and other activities.
- Students understand and follow the Online Safety Policy and acceptable use policies.
- 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/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.
- They should act as good role models in their use of digital technologies, the internet and mobile devices
- Recognising SEND Needs in Online Safety Education, and that a one-size-fits-all approach is not appropriate—teaching must be personalised or contextualised for:
    - Pupils with SEND
    - Pupils who have experienced abuse or trauma
    - SEND pupils may face heightened online risks, such as:
        - Difficulty recognising grooming or manipulation
        - Increased vulnerability to cyberbullying
        - Challenges in understanding privacy and consent

Students:

- Are responsible for using GHES's digital technology systems in accordance with the student acceptable use agreement.
- 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 school and realise that GHES'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. GHES will take every opportunity to help parents understand these issues through parents' bulletin, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support GHES in promoting good online safety practice and to follow guidelines on the appropriate use of:

Awareness of Online Risks

- Parents should understand the 4 Cs of online risk:
  Content – harmful or misleading material (e.g. misinformation, conspiracy theories)
  Contact – inappropriate or exploitative interactions
  Conduct – risky or harmful online behaviour
  Commerce – scams, fraud, and exploitative advertising

Supporting Safe Technology Use at Home

- Monitor and guide children's use of devices, apps, and platforms.
- Use parental controls and privacy settings to reduce exposure to harmful content.
- Encourage open conversations about online experiences and concerns.

Partnership with Schools

- Engage with school-led online safety initiatives (e.g. workshops, newsletters).
- Support the school's filtering and monitoring policies by reinforcing safe practices at home.
- Report concerns to the school if a child experiences online harm or distress

Promoting Critical Thinking

- Help children question what they see online, especially AI-generated content or misinformation.
- Encourage children to verify sources and think critically about digital media

Data Protection and Privacy

- Teach children not to share personal information online.
- Be aware of how AI tools and apps may collect or misuse data.

Staying Informed

- Stay up to date with school policies and national guidance on online safety.
- Make use of resources shared by schools that signpost support, advice and guidance.

Policy Statements

Education – Students

Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. 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/digital literacy is therefore an essential part of GHES's online safety provision predominantly sits within the PSHE Curriculum. However, as over 50% of the delivery of teaching at GHES is carried out online, reinforcing online safety is found in all other curriculum areas – where there is planned reference and opportunity to teach aspects of online safety woven into topics.

The following outlines all of the aspects GHES covers:

- Critical Thinking & Media Literacy
  - How to identify misinformation, disinformation, and conspiracy theories
  - Skills to question online content, challenge harmful narratives, and avoid manipulation

- Safe Online Conduct
  - Respectful behaviour online, including avoiding cyberbullying, trolling, and peer-on-peer abuse
  - Understanding the risks of sharing personal or inappropriate content (e.g. sexting)
  - How to report concerns or harmful behaviour online

- Responsible Use of AI and Technology
  - Awareness of risks from AI-generated content, including bias and inappropriate material
  - Understanding data privacy and the importance of not sharing personal information with AI tools
  - Ethical use of digital tools and platforms

- Privacy and Security
  - How to protect personal data and use privacy settings
  - Recognizing and avoiding online scams, phishing, and unsafe websites
  - Importance of strong passwords and secure accounts

- Online Relationships and Contact Risks
  - How to stay safe when interacting with others online
  - Recognizing signs of grooming, exploitation, or radicalisation
  - Knowing when and how to seek help from trusted adults

- Curriculum Integration
  - Online safety is taught through PSHE
  - Schools should tailor content to meet the needs of vulnerable pupils, including those with SEND or who have experienced abuse

- Filtering and Monitoring Awareness
  - Students should understand that school systems are monitored for safety
  - They should know what is acceptable use of school devices and networks

- Where relevant, Link Tutors ensure families complete the family agreement form to encourage open dialogue about online safety.
- Key online safety messages are reinforced through the work of the online safety group and their communication with staff, students and parents.
- 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.
- 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.
- 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 if in GHES outpatients. The Learning Technologist is able to give access to such sites if planned in advance and approved by the DSL for the period of the lesson. If the website access is required in the home, we would inform parents beforehand to review risks, and supervision, before suggesting the use of it to the student.

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.

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

- The initial visit
- Link Tutors – includes use of parents checklist and family agreement.
- The Learning Technologist.
- The Link Tutor and online induction session taken by the Learning Technologist.
- Curriculum activities.
- Practical Resources through letters, newsletters, web site, learning platform, parent bulletin.
    - Share guidance documents, toolkits, and links to trusted websites (e.g. Childnet, Internet Matters, NSPCC).
    - Offer tips on parental controls, privacy settings, and safe app usage.
    - Include AI-related risks, such as inappropriate content generation or data sharing
- Regularly communication through newsletters, emails, and our learning platform:
    - Share updates on online safety trends
    - Promote safe digital habits
    - Alert parents to new risks or incidents
- Parents/carers sessions.
- High profile events/campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites/publication.

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:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school 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 Group, Learning Technologist and DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The online safety Group, Learning Technologist and/or DSL will provide advice/guidance/training to individuals as required.

Training – Management Committee

Management Committee members should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided through Gloucestershire Safeguarding Children's Partnership (GSCP).
- Participation in GHES training sessions.

Technical – infrastructure/equipment, filtering and monitoring

To ensure all students at GHES are able to access their learning either through online lessons, or face to face lessons in the home or at GHES outpatients, we have the following in place:

- Students can access online lessons whilst at home using their own device(s.)
- Where students can access online lessons from their home but do not have their own device, we will provide them with a GHES curriculum laptop.
- A curriculum network at GHES outpatients and in Gloucester Royal Hospital (GRH) schoolroom. Any student participating in lessons in these locations is expected to use the GHES curriculum network when online.

GHES will be responsible for ensuring that the curriculum 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. *Ref: GHES ICT Technical Policy*

GHES is not able to fully monitor what goes on individual homes in terms of the filtering systems in place, and the monitoring by parents. Therefore during initial visits case managers and link tutors will discuss and provide literature to parents and students on the safe use of digital technology. All students and their parents are required to read and sign the Acceptable Use Agreement.

For the GHES Curriculum network:

- GHES technical systems will be managed in ways that ensure that the school meets recommended technical requirements. *Ref: Online Safety Audit*

- There will be an annual–review and audit of the safety and security of technical systems being used. *Ref: Online Safety Audit*
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to the technical systems and devices.
- All users of the GHES curriculum network (staff and students) will be provided with a username and secure password by the Learning Technologist 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 GHES systems, used by the Learning Technologist must also be available to the Head of Service or other nominated senior leader and kept in a secure place.
- The Learning Technologist 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 through Smoothwall. Illegal content (child sexual abuse images) is filtered by the 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.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, 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 devices are protected by up-to-date virus software.
- An acceptable use policy is in place regarding the extent of personal use that users (staff/students) and their family members are allowed on school devices (GHES curriculum laptops) that may be used out of school.

Mobile Technologies

Mobile technology devices may be school owned/GCC provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the GHES curriculum 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 of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices 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 school's online safety education programme.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.
- Where laptops are loaned to students, an acceptable use and agreement policy is put in place. All laptops are re-set back to original curriculum settings before they are loaned out to ensure no personal data or information remains on them from the previous student. This is carried out by the Learning Technologist.

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/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images 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. *Ref: Student and Staff AUPs*
- Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press when a student's referral to GHES is accepted.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow the school's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on GCC/GHES 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 GCC / GHES 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' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student/pupil and parents or carers.

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:

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

- The official ...@ghes.gloucs.sch.uk email service may be regarded as safe and secure. Users should be aware that email communications are monitored. All email communication between staff and students must use this domain name.
- Users must immediately report to the Head of Service 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.

Social Media - Protecting Professional Identity

GHES 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.

Staff should ensure that:

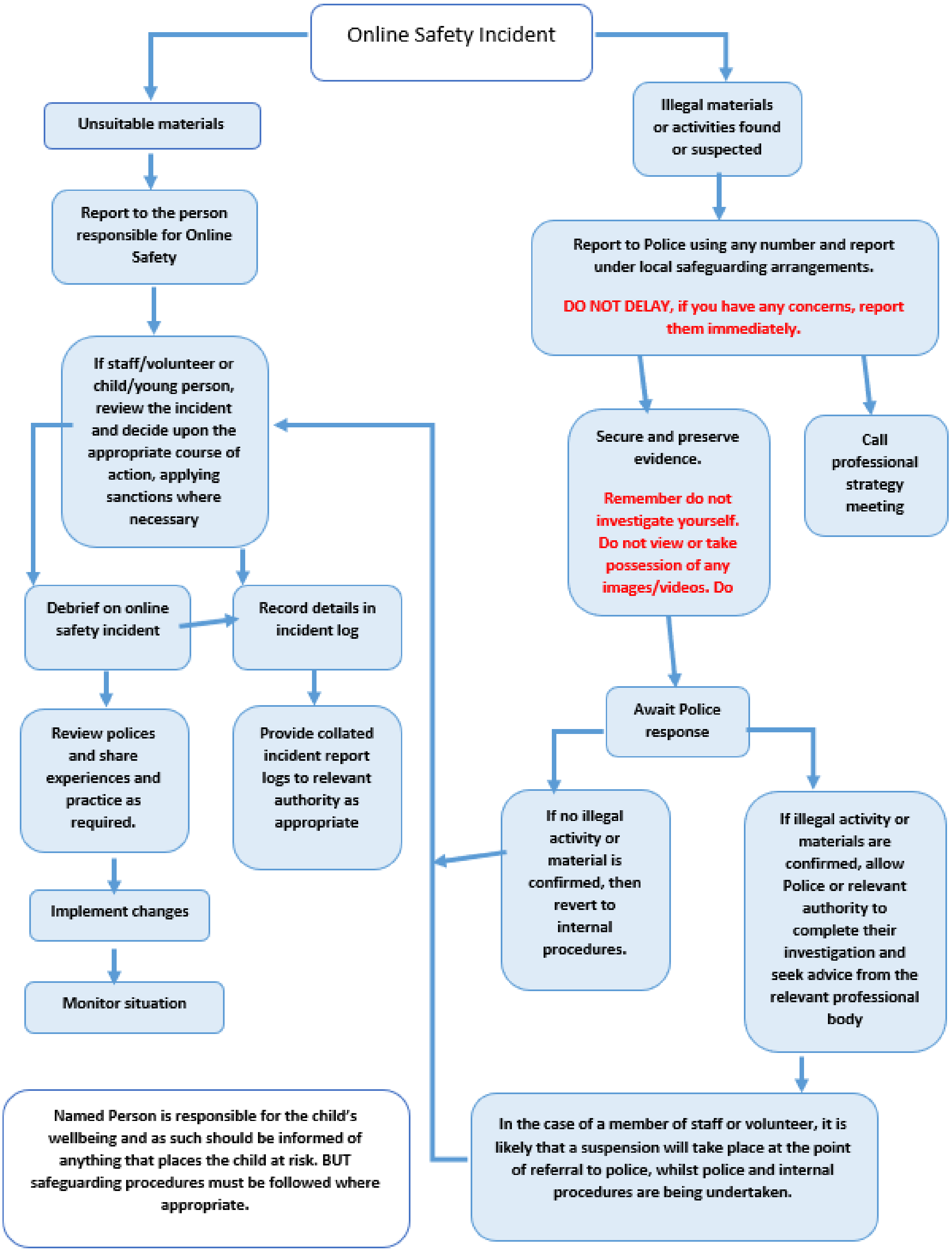
- No reference should be made in social media to students, parents/carers or GHES staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the GCC or GHES.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await 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

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Other Incidents

It is hoped that all members of the GHES community will be responsible users of digital technologies, who understand and follow the 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 and include the DSL. 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.
- 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, 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 and Gloucestershire MASH hub 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
    - child sexual exploitation (CSE)

- **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 school 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.

GHES actions & sanctions

It is more likely that GHES 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:

- Refer to Head of Service and where appropriate LADO
- Informing parents immediately
- Determining any appropriate sanctions
- Review of training / learning requirements for an individual
- Contact with MASH (safeguarding concern)
- Contact with police

FOR STAFF AT GHES:

Polices that should be read in conjunction with this, available through GCC staffnet:

Staff Acceptable Use Policies | Gloucestershire County Council https://www.gloucestershire.gov.uk/council-and-democracy/strategies-plans-policies/information-management-and-security-policies/

Sections that should be read:

Staff Acceptable Use Policies

- Remote access policy
- BYOD Policy
- M365 Acceptable Use Policy
- Information IT Access Policy
- ICT and Equipment policy
- Remote Working (IMS) Policy
- Social Media Policy
- Password Policy
- Internet and Digital communications policy
- Generative AI Policy
- WhatsApp Business Case policy
- CANVA Business Case

Appendices

1. Allegations Management
2. Online Safety Audit – being completed during 2025/26 Term 2
3. Online Technical Policy – to be updated following Online Safety Audit 2025/26 Term 2
4. Acceptable Use Agreement KS2 - updated
5. Acceptable Use Agreement KS3 & KS4 - updated
6. Family Agreement – used by Link Tutors
7. Consent Forms – give in parent pack
8. E-safety family check – used by Link Tutors
9. AI Classroom Poster
10. Education for Students – table of how we cover this.