BHASVIC

ONLINE SAFETY POLICY

Last Updated: November 2025

Review Date: November 2026

BHASVIC

ONLINE SAFETY POLICY

Contents

1. Policy Overview

- BHASVIC recognises that online safety is an essential part of child protection and safeguarding and acknowledges its duty to ensure that all students and the college community are protected from potential harm and inappropriate material online. The college believes that students should be empowered to build resilience and to develop strategies to manage and respond well to online risk.

- This policy is written in line with *Keeping Children Safe in Education 2025* (KCSIE), 'Teaching Online Safety in Schools,' and other statutory documents. It is supplemented by a series of related acceptable use agreements and college policies, including the Safeguarding and Child Protection Policy, and has been developed by the BHASVIC Online Safety Group.

Our college aims to:

- Build an infrastructure of online safety, through providing appropriate filtering and monitoring on college devices and networks and regularly review their effectiveness.
- Develop an effective culture of online safety and embed an integrated approach that empowers educational professionals to safeguard and educate the college community on our rights and responsibilities in use of technology, including mobile and smart technology.
- Have robust processes in place to ensure the online safety of students, staff, volunteers, and governors, establishing clear mechanisms to identify, intervene, escalate any concerns, and record the misuse of digital technologies and online safety incidents.
- Collaborate with parents/carers and external agencies, to empower students to safely use technology, including the internet, mobile and smart technology, as an essential tool for life-long learning.
- Identify and support groups of students that are potentially at greater risk of harm online than others and provide equal protection within our college community from all types of harm or abuse for all children and young people, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation.

The four key categories of risk

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk (*KCSIE 2025*):

- **Content** – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as

children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct** – online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

2. Policy Scope

- The policy applies to all members of the college community, including staff, students, governors, and other college users, including visitors, volunteers, contractors.
- The policy applies to all internet access and use of technology, including personal devices, or where students, apprentices, staff, or other individuals have been provided with college issued devices for use off-site, such as work laptops, tablets, or mobile phones.

3. Policy Purpose

The purpose of this policy is to:

- Set expectations for the safe and responsible use of digital technologies for learning, administration, and communication, to ensure that the safety and wellbeing of our college community is paramount when adults, young people or children are using the internet, social media, or mobile devices.
- Provide staff, governors and volunteers with the overarching principles that guide our approach to online safety, establishing guidance and training in the responsible use of digital technologies, and how to utilise this understanding in the planning of curriculum, tutorial and other learning opportunities, to help safeguard learners in the digital world.
- Ensure that as an organisation we operate in line with our values and within the law in terms of how we use online devices.

4. Monitoring and Review of Policy

- The policy will be reviewed annually and will be under continuous revision in response to significant new developments and trends in technology, new threats to online safety or incidents that have taken place.

5. Roles and Responsibilities

- All members of the college community have a key role to play with regards to online safety. The following sections outline the online safety roles and responsibilities of individuals and groups within the college:

Role	Responsibility
Principal and Senior Leadership Team	• The Principal has a duty of care for ensuring the safety (including online safety) of members of the college community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in *KCSIE*. • The Principal 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 online safety allegation being made against a member of staff. • The Principal/senior leaders are responsible for ensuring that the Designated Safeguarding Lead/Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant. • The Principal/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in college who conduct the internal online safety monitoring role. • The Principal/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead/Online Safety Lead. • The Principal/senior leaders will collaborate with the responsible Governor, the Designated Safeguarding Lead (DSL) and deputies (DDSLs) and IT service providers in all aspects of filtering and monitoring.
Governors	• Governors are responsible for the approval of the Online Safety Policy. • A member of the governing body will take on the role of Safeguarding governor to include: o Regular meetings with the Designated Safeguarding Lead and Deputies/Online Safety Lead o Checking that the Online Safety Policy is fit for purpose o Checking that provision outlined in the Online Safety Policy is taking place as intended. • Ensuring that the filtering and monitoring provision is reviewed at least annually. The review will be conducted by members of SLT,

	the DSL, and the IT service provider and involve the responsible governor- in-line with the DfE Filtering and Monitoring Standards • Receive training on safe internet use, cyber-security, and online safeguarding issues as part of safeguarding training. • The governing body will also support the college in encouraging parents/carers and the wider community to become engaged in online safety awareness.
Designated Safeguarding Lead and Deputies	• The Designated Safeguarding Lead takes lead responsibility for safeguarding and child protection, including online safety, and has the relevant knowledge and capability required to keep our students safe whilst they are online at college. **The DSL/DDSL's will:** o Undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge about online safety, cyber security, data protection, and Prevent, at regular intervals, to enable them to understand the risks in how digital technologies are used and are developing, regarding the areas defined in KCSIE: content, contact, conduct, commerce. o Ensure that safeguarding reports are submitted at half termly SMT Business meetings, which includes data on filtering and monitoring alerts, and online safety incidents. o Receive reports of online safety incidents and decide whether to make a referral by consulting with relevant agencies, ensuring that all incidents are recorded. o Consult with staff and IT providers on matters of safety, safeguarding and welfare, including online and digital safety. o Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents to the Safeguarding Leads.
Online Safety Lead	• While the responsibility for online safety is held by the DSL, the college has appointed an Online Safety Lead (DDSL) to work in support of the DSL in carrying out these responsibilities, including: o Lead the Online Safety Group. o Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), and deputies (DDSLs), being aware of the potential for serious child protection concerns. o Ensure that online safety incidents are logged to inform future online safety developments.

	○ Have a leading role in establishing and reviewing the college online safety policies. ○ Promote an awareness of and commitment to online safety education and awareness raising. ○ Provide (or identify sources of) training and advice for staff/governors/parents/carers/students. ○ Consult with (college/local authority/external provider) technical staff, pastoral staff, and support staff as relevant. ○ Receive regular updates through training sessions and by reviewing online safety newsletters from external statutory agencies and disseminate guidance and training opportunities for staff.
Curriculum and Support Staff	• Heads of Student Support, Experience and Guidance, and Curriculum staff will work with the Online Safety Lead to develop online safety education. This will be provided through: ○ The BHASVIC tutorial programme ○ Enrichment activities and events ○ Student conferences ○ Relevant national initiatives and opportunities e.g. Safer Internet Day. ○ Student Online Safety Ambassador programmes Staff are responsible for ensuring that: • They have an awareness of current online safety matters/trends and of the current college Online Safety Policy and practices. • They understand that online safety is a core part of safeguarding. • They have read, understood, and signed the Staff Acceptable Use Policy (AUP). • They immediately report any suspected misuse or problem to the Safeguarding Team for investigation/action, in line with the college safeguarding procedures. • All digital communications with learners, parents/carers and external agencies are on a professional level and only conducted using official college systems, such as college email or Microsoft Teams. Personal email and social media must not be used for these communications. • Ensure learners understand and follow the Online Safety Policy and acceptable use agreements. • They monitor the use of digital devices connected to the college network.

	• In lessons where internet use is necessary, learners are advised regarding responsible online search activity. • They model safe, responsible, and professional online behaviours in their own use of technology, including outside of work and in their use of social media. • Incidents of online bullying, sexual harassment, discrimination, hatred, abuse, extremist or radical views, must be reported to the Safeguarding Team urgently and recorded via CPOMS in accordance with our Prevent Duty and Safeguarding and Child Protection Policy and procedures.
Head of IT, Technical Staff, and IT Provider	The Head of IT and IT Provider work with the Senior Leadership Team and the Designated Safeguarding Lead to ensure that: o They are aware of and follow the college Online Safety Policy to carry out their work effectively. o The college technical infrastructure is secure and is not open to misuse or malicious attack. o The college meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority or other relevant body. o There is clear, safe, and managed control of user access to networks and devices. o They keep up to date with online safety technical information to effectively conduct their online safety role and to inform and update others as relevant. o The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Safeguarding Team for investigation and action. o The filtering software is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person. o Ensure that monitoring software is implemented and regularly updated. Ensure that annual filtering and monitoring checks are conducted.
Online Safety Group	• The Online Safety Group provides a consultative group that has wide representation from the college community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy, including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.

	The Online Safety Group consists of the following members: • Designated Safeguarding Lead • Online Safety Lead • Senior Leaders • Technical and IT staff • Curriculum/Teaching staff • Support staff Members of the Online Safety Group will assist the DSL/DDSLs/Online Safety Lead, and other relevant staff with: o The production/review/monitoring of the college Online Safety Policy and associated documents. o Requests for filtering changes. o Mapping and reviewing the online safety education provision – ensuring relevance, breadth, and progression and coverage. o Reviewing network/filtering/monitoring/incident logs, where possible. o Encouraging the contribution of learners to staff awareness, emerging trends, and the college online safety provision. o Consulting stakeholders – including staff/parents/carers about the online safety provision. o Monitoring improvement actions identified through use of the 360-degree safe self-review tool. o Consulting with students regarding the shaping of online safety strategy, canvassing feedback, student contributions to online safety education, events, policy, and protocols.

6. Students, Parents and Carers and Community Users:

- Students, parents, carers, and community users who access college digital technology systems, (including on personal devices) will be expected to:

  - Adhere to Acceptable Use of IT agreements, and report abuse, misuse, or access to inappropriate materials urgently to the Safeguarding Team or college staff.

  - If a student or someone they know feels vulnerable when using online technology, they should report concerns to the Safeguarding team or college staff.

- Understand the importance of adopting good online safety practice when using digital technologies and realise that the college's Online Safety Policy also covers their actions outside of college.

- Parents and carers play a crucial role in ensuring that their young people understand the need to use the online services and devices in an appropriate way. Parents and carers will be encouraged to support the college in reinforcing the online safety messages provided to learners in college, including the safe and responsible use of IT.

- The college will raise parents/carers' awareness of internet safety in newsletters or other communications, and in information via our website. This policy will also be shared with parents/carers via the college website.

- The college will let parents/carers know what systems the college uses to filter and monitor online use.

- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL/DDSLs.

- The college encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge with the wider community.

7. Contribution of Students:

- BHASVIC acknowledges and uses the skills and knowledge of students in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the college community and how this contributes positively to the personal development of young people.

- Their contribution is recognised through:

    - Mechanisms to canvass student feedback and opinion, including student voice.
    - Students designing/updating acceptable use agreements.
    - Contributing to online safety events with the wider college community.
    - Opportunities to engage in Online Safety Ambassadors Programmes (e.g. Breck Online Safety Ambassadors)

8. Online Safety Education:

- BHASVIC will provide education for students in online safety by embedding learning throughout the tutorial programme, Personal Development workshops with external visitors, curriculum, peer education, and awareness raising events such as Safer Internet Day.

- Key online safety messages are reinforced through advice and information on SharePoint, our website, and via online platforms such as the myBHASVIC app.

- Students can access information on seeking support for a range of safeguarding issues, on the Student Services Hub SharePoint site, which includes advice regarding how to access support for a wide range of safeguarding concerns linked to Online Safety, for example, how to seek support for harms encountered online such as sexual harassment, bullying, sharing of indecent images.

- During the induction process at the start of the new academic year, all students are expected to read and adhere to the IT Acceptable Use Policy and the Student Code of Conduct. These, and all associated policies, are accessible via the college website and SharePoint sites.

- All students are informed that network and internet usage will be monitored for safety and security purposes in accordance with relevant legislation.

Students will be supported to understand:

- How changes in technology affect safety, including new ways to protect their online privacy and identity.

- How to identify harmful behaviours online (including bullying, cyberbullying, abuse, or harassment) and how to report or find support if they have been affected by those behaviours or any other online safety concerns.

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material. Not to provide material to others that they would not want shared further and not to share personal material that is sent to them.

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours and can negatively affect behaviour.

- That sharing and viewing indecent/abusive images of children (including those created by children) is a criminal offence that carries severe penalties including imprisonment.

- The safe use of social media and the internet will also be covered where relevant. Students are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information, including understanding how misinformation, disinformation (including fake news) and conspiracy theories are harmful.

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Vulnerable Learners

- BHASVIC recognises that some students are more vulnerable online due to a range of factors, such as, being in care, care leavers, having special educational needs and disabilities (SEND), having mental health needs, having English as an additional language (ESOL), and those who have experienced trauma or loss.

- Where necessary, when implementing online safety education, specialist support will be sought from staff, including those responsible for safeguarding, mental health and SEND.

9. Training and Engagement with Staff

- All new and existing staff receive appropriate annual safeguarding and child protection training and updates, including online safeguarding issues such as, data protection, safe internet use, cyberbullying, and the risks of online radicalisation.

- Staff are reminded to adopt professionalism regarding codes of conduct and acceptable use of college systems and devices, and of social media. New and existing staff are made aware that IT systems are monitored, and activity can be traced back to individual users.

- All staff will be made aware that technology is a significant component in a wide range of safeguarding and wellbeing issues, and that children and young people are at risk of online abuse.

  Children and young people can abuse their peers online through:

  - Abusive, threatening, harassing and misogynistic messages.
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos.
  - Sharing of abusive images and pornography.
  - Physical abuse, sexual violence, and initiation/hazing type violence.

- Training will help staff to ensure students can recognise dangers and risks in online activity, understand procedures for reporting and addressing online safety concerns, and locate resources and tools to use with students in online safety education and interventions.

10. Online Safeguarding Concerns

- Our Safeguarding and Child Protection Policy provide staff with guidance on types of abuse, how to spot signs of abuse, how children and young people can abuse their peers, and how to report issues including:

- **Cyberbullying**

  Cyberbullying takes place online, such as through social networking sites, messaging apps, or gaming sites. It is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

- **Sexting (Sharing of nude and/or semi-nude images)**

  The college will follow UKCIS advice on how to respond to any incident of sexting. We will provide appropriate support for sexting incidents which take place in and out of college. Within college, any device which has an illegal image of a child under eighteen, or is suspected of having such an image, will be secured and switched off.

- **Child on Child Sexual Violence and Sexual Harassment**

  All staff are made aware that sexual violence and sexual harassment can occur between children of any age and gender and can include online harassment.

  Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include, non-consensual sharing of sexual images and videos, sexualised online bullying, unwanted sexual comments, and messages, including, on social media, and sexual exploitation, coercion, and threats.

- **The Prevent Duty**

  The college works to ensure students are safe from terrorist and extremist material when accessing the internet on the premises. We are subject to a duty under section 26 of the *Counter-Terrorism and Security Act 2015*, in the exercise of their functions, to have "due regard to the need to prevent people from becoming terrorists or supporting terrorism".

  Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism, as informed by our risk assessment. Appropriate monitoring of internet use will identify attempts to access such material. Students are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

  The online monitoring system alerts Safeguarding Leads to concerning content shared by students via college Wi-Fi in Teams chat or Microsoft Office documents, and Prevent concerns are monitored and responded to with appropriate interventions.

11. Reporting and Responding to Online Safety Incidents

- BHASVIC will take all reasonable precautions to ensure online safety for all users and recognises that incidents may occur inside and outside of the college, which will need intervention. It is more likely that the college will need to deal with incidents that involve inappropriate rather than illegal misuse.

  The college will ensure:

  - There are clear reporting routes which are followed by all members of the college community which are consistent with safeguarding procedures, including logging incidents on CPOMS, which automatically alerts Safeguarding Leads, or calling the Duty phone for urgent response.

- The Designated Safeguarding Lead and Deputies will be informed of online safety incidents involving child protection concerns, which will be escalated in accordance with safeguarding, Acceptable Use of IT and Code of Conduct procedures.

- Where there is cause for concern or reason to believe that illegal activity has taken place or is taking place then the college Safeguarding Leads will escalate the concern to the police and statutory external agencies as appropriate.

  Illegal activity or the potential for serious harm, may include:

  - Non-consensual images
  - Self-generated images, including images generated via AI
  - Terrorism/extremism
  - Hate crime/Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy
  - Cybercrime

12. Examining electronic devices

- The Principal and any member of staff authorised to do so by the Principal can conduct a search and confiscate any electronic device that they have reasonable grounds for suspecting that it:

  - poses a risk of harm to staff or students,
  - and/or may undermine the safe environment of the college or disrupt teaching,
  - and/or evidence in relation to an offence.

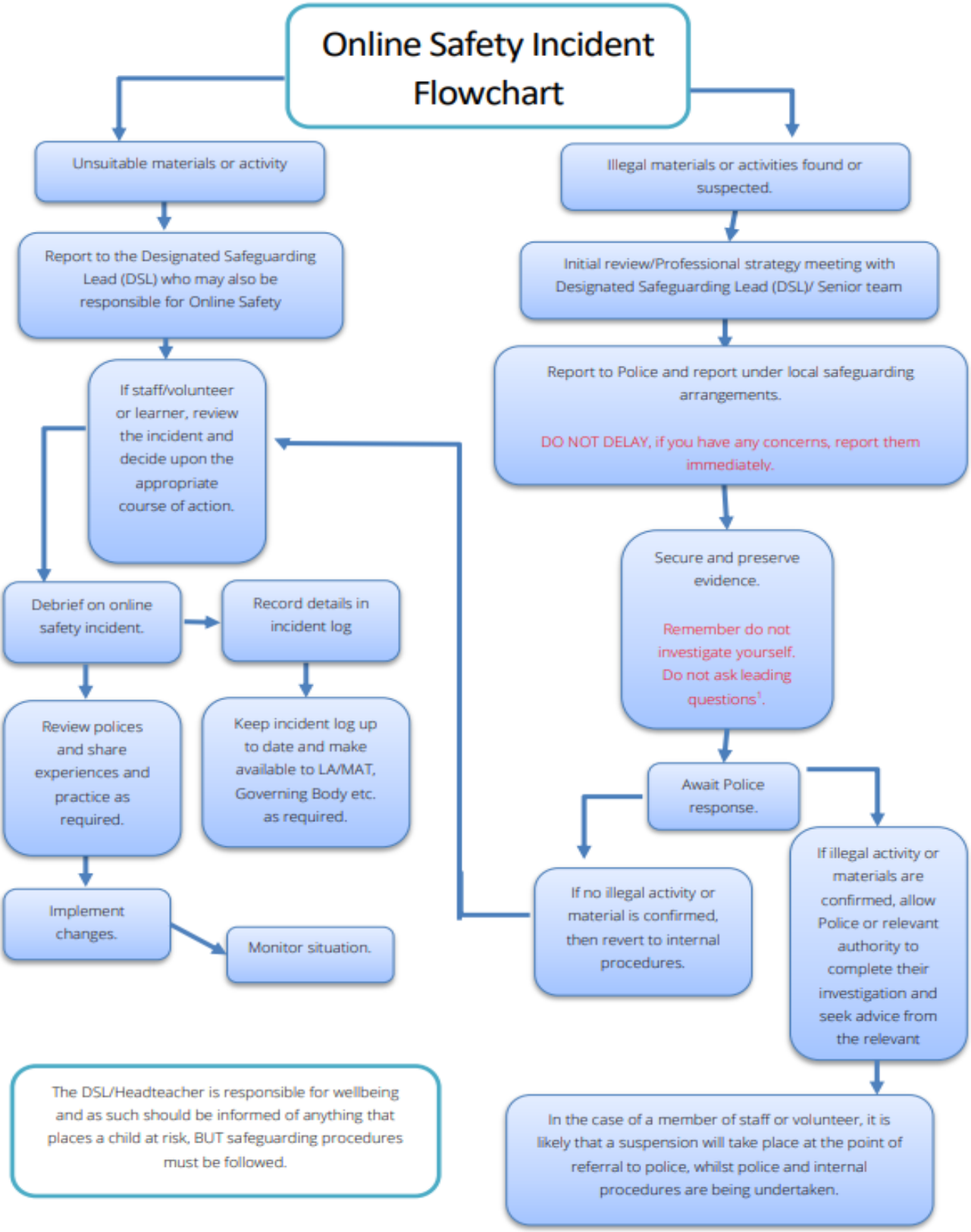
- If a staff member **suspects** a device **may** contain an indecent/abusive image of a child (also known as a nude or semi-nude image), they will:

  - **Not** view the image.

  - Confiscate the device and report the incident to the DSL/DDSL immediately, who will decide what to do next, following appropriate guidelines, as necessary.

  - The DSL/DDSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

13. Online Safety Incident Flowchart



14. Filtering and Monitoring – Systems and Standards

- BHASVIC protects users and college systems using a blend of strategies to manage access to content on all devices using the college's internet provision, to limit exposure to online risk.

- These include, physical monitoring (e.g. adult supervision in the classroom), filtering of internet access through an external provider, and a third party assisted proactive technology-based monitoring service.

- The external technology providers are aware of our Online Safety and Acceptable Use of IT Policies, and we have a Data Processing Agreement in place, including a Data Protection Impact Assessment (DPIA), to ensure that the filtering and monitoring strategy is integrated alongside our relevant data sharing agreements.

- BHASVIC adheres to filtering and monitoring standards and guidance as defined by the Department for Education (DfE) and the UK Safer Internet Centre.

    - We have identified and assigned roles and responsibilities to manage filtering and monitoring systems.

    - We review, check, and agree filtering and monitoring provision and policy at least annually and it is updated in response to changes in technology and patterns of online safety incidents and safeguarding risks.

    - We block harmful and inappropriate content without unreasonably impacting teaching and learning, and there are effective routes for users to report issues.

    - We have effective filtering and monitoring strategies in place, and we manage access to content across our systems for all users.

15. Filtering

- The automatic web filtering blocks network access to specific websites, network resources, and IP addresses:

    - That are known to propagate malware, facilitate the compromise of sensitive or personal data, or otherwise pose an information security threat.

    - That provide or facilitate access to illegal content (e.g. child sexual abuse images), in accordance with our Safeguarding and Child Protection Policy and updated guidance from the Internet Watch Foundation.

    - That provide or facilitate access to harmful content and extremist ideas that are part of terrorist ideology, in accordance with the college's Prevent Duty and risk assessment, and updated guidance from the Police and Home Office.

- Filtering logs are regularly reviewed and analysed by the IT Team, alerts are prioritised for intervention by the Safeguarding Leads, and indications of potential harm are acted upon.

- Staff and students wishing to view material on external websites whose access has been disabled by targeted filtering should request access through the IT Support department.

- The Designated Safeguarding Lead will moderate requests. No attempt should be made to circumvent the filters.

16. Monitoring

- Online activity suspected as inappropriate or harmful, via all platforms on the college network such as email, Teams chat, and websites, are swiftly detected.

- Keywords and other indicators are actively monitored across devices on the college network. This draws attention to concerning behaviours, communications, or access.

- Alerts are managed by a specialist third-party provider and sent to the Safeguarding Team (DSL/DDSLs). Safeguarding Leads act on alerts that signal potential harm and provide rapid interventions to protect users.

- For information security purposes, telephone and computer systems (including email and online communication platforms such as Microsoft Teams), and any personal use of them, may also be continually monitored by automated systems. This is for the purpose of, the effective and efficient planning and operation of the IT facilities, detection, mitigation and prevention of cyber security threats, detection, and prevention of infringement of these and other policies and regulations, investigation of alleged misconduct, and to comply with any legal obligation.

  Monitoring Content

- Recognising that no monitoring can be guaranteed as 100% effective, our monitoring strategy ensures that we at least cover the following content:

  - Illegal
  - Bullying
  - Child Sexual Exploitation
  - Discrimination
  - Substance Use
  - Radicalisation and Extremism
  - Gambling
  - Hate Speech
  - Pornography
  - Self-Harm
  - Suicide
  - Violence

17. Technical Security and Cybersecurity

- The Acceptable Use of IT Policy provides guidelines for users in how to safely access college technical systems. The college technical systems will be managed in ways that ensure that the college meets recommended technical requirements.
    - All users have clearly defined access rights to college technical systems and devices.
    - Password policy and procedures are implemented and allocated with a risk-based approach.
    - Servers, wireless systems, and cabling are securely located, and physical access restricted.
    - Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, and devices from accidental or malicious attempts which might threaten the security of the college systems and data. These are assessed regularly. The college infrastructure and individual workstations are protected by up-to-date endpoint software.
    - There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
    - The IT Manager is responsible for ensuring that all software purchased by and used by the college is adequately licenced and that the latest software updates are applied.
    - An appropriate system is in place for users to report any actual/potential technical incidents or security breaches to the relevant person, as agreed.
    - Use of college devices outside of college is regulated by an Acceptable Use statement that a user consents to when the device is allocated.
    - Personal use of any device on the college network is regulated by Acceptable Use statements that a user consents to when using the network.
    - Staff members and governors are not permitted to install software on college-owned devices without the consent of SLT/IT service provider.
    - Removable media is not permitted unless approved by SLT/IT service provider.
    - Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
    - Mobile device security and management procedures are in place (where mobile devices access college systems).
    - Guest users are provided with appropriate access to college systems based on an identified risk profile.

- Staff and students are briefed on how to identify suspicious links and reporting mechanisms for alerting relevant staff to suspicious online activity.

18. Mobile Technologies:

- The Acceptable Use of IT Policy outlines in further detail our policy on BYOD (Bring Your Own Device) and includes guidelines for safely accessing college systems when using personally owned devices such as, tablets, smartphones, laptops, and PCs.

- Any use of mobile devices in college by students, staff and governors must be in line with the acceptable use agreement. Any breach of the Acceptable Use Agreement may trigger disciplinary action in line with relevant Codes of Conduct.

- A wide range of communication technologies increases effective administration and has the potential to enhance learning.

- Although our online monitoring software picks up potential safeguarding issues via activity on mobile devices using college networks, students will have access to mobile phone networks that are not monitored by our online monitoring software systems.

- To safeguard our college community in the use of mobile devices, we provide online safety training and education to enable students and staff to make safe and informed choices regarding their internet usage and social communications.

19. Social Media:

- With widespread use of social media for professional and personal purposes this policy aims to set out clear guidance to manage risk and behaviour online and includes the protection of students, the college, and the individual, when publishing any material online.

- Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust, and that their conduct should reflect this.

- All colleges and local authorities have a duty of care to provide a safe learning environment for students, staff, and the college community.

  The college will:

  - Encourage staff to assess sites before use and check the site's terms and conditions to ensure the site is age appropriate, and whether content can be shared by the site or others without additional consent being given.

  - Ensure that departmental blogs, advice, guidance and messaging via learning platforms and college databases are password protected and ensure that any digital communication between staff and students or parents and carers, is open, transparent, and professional in tone and content.

- Raise awareness of the personal use of email, online learning platforms, social networking, social media, and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour online.

- Ensure that staff and governors are advised that no reference should be made to students, parents/carers, or college staff on their personal social networking accounts.

- Report to the Safeguarding Team any concerns regarding inappropriate use of email, social networking, social media, and personal publishing sites.

- Provide education, guidance, and training for the college community, including parents/carers, in the safe and acceptable use of social media, acceptable use, age restrictions, digital and video images, checking settings, data protection and reporting issues.

- In the event of any social media issues being found that do not comply with relevant policies, alongside relevant external support, advice may be sought from the Professionals Online Safety Helpline.

20. Digital Images, Videos and Sound:

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant access to images that they may have recorded themselves or downloaded from the internet.

- However, students, staff, governors, and parents/carers need to be aware of the risks associated with publishing digital images on the internet.

- It is common for employers to conduct internet searches for information about potential and existing employees.

- Photographs, video, and sound recorded within college are used to support learning experiences across the curriculum, to share learning with parents/carers on our learning platforms, and to provide information about the college on the website.

  The college will:

  - Build a culture where permission is always sought before a photograph is taken or video and sound are recorded; including encouraging students to seek permission from other students to take, use, share, publish or distribute images and sound.

  - Ensure verifiable and relevant permissions are obtained before images, sound recordings or videos of students are electronically published on the college website, on social media, or in the local press.

  - Any written consent, where students' images, video and sound are used for publicity purposes, is kept until the data is no longer in use.

- When using digital images, staff educate students about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.

- Allow staff to take images, record video, and sound on college equipment to support educational aims, following the college policy regarding the sharing, distribution, and publication of those.

- Ensure that images, sound, or videos that feature students will be selected carefully with their knowledge, and that students represented are not participating in activities that might bring the individuals or the college into disrepute.

- Make adults and young people aware of the risk that any published image, video and sound could be reused and repurposed.

- Only hold digital/video images on college approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with data protection.

- Make clear to professional photographers who are engaged to record any events or provide a service, that they must work according to the terms of the Online Safety and Safeguarding & Child Protection Policies. They will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to necessary consents.

21. Online Publishing:

- The college communicates with parents/carers and the wider community and promotes the college through the public-facing website, social media, online newsletters, and college databases.

- The college ensures that Online Safety Policy has been followed in the use of online publishing, e.g., use of digital and video images, copyright, identification of young people, publication of calendars and personal information – ensuring that there is least risk to members of the college community through such publications.

- Where learner work, images or videos are published, their identities are protected, and full names are not published unless consent is provided.

The college will:

- Ensure that the college community uses secure business systems for communication and that personal information is not sent via unsecure systems.

- Ensure that any digital communication between staff and students or parents/carers is professional in tone and content.

- Make users aware that communications are monitored by the college.

- Inform users what to do if they receive online communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

- Advise students about email and other communication tools alongside safe, healthy, and appropriate use of technology, in accordance with the Acceptable Use Policy.

- Embed education regarding online safety issues throughout curriculum and pastoral schemes of work.

- Only publish official staff email addresses where required.

22. Use of personal devices:

The college will:

- Ensure that staff and students understand that the Acceptable Use and Codes of Conduct policies will apply to the use of their own portable device for college purposes.

- Inform staff and visitors that they are not allowed to use personal devices to take photographs or video in college for any purpose.

- Advise staff not to use their personal mobile phone to contact students, parents and carers and provide a mobile phone or 3CX access for activities that require them to do so.

- Challenge staff and visitors when there is suspected misuse of mobile phones or device.

- Use the right to collect and examine any student device that is suspected of containing offensive, abusive, or illegal content, or is suspected of causing issues on the college internet connection.

23. Staff and governors using work devices outside of college:

- Staff members and governors must not use the device in any way that would violate the college's terms of acceptable use as outlined in our Acceptable Use of IT Policy. Work devices must be used solely for work activities.

- Users will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

    - Keeping the device password-protected – strong passwords are at least eight characters, with a combination of upper and lower-case letters, numbers, and special characters.

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

- If staff, students, or governors have any concerns over the security of their device, they must seek advice from the IT Services Manager.

24. Assessment of risk

- Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the college will examine and adjust the Online Safety Policy. Part of this consideration will include looking into the educational benefit of the technology alongside assessing the risk of access to inappropriate material.

- The college provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a college device.

- All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence and breaches will be reported.

25. Artificial Intelligence

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students, and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Copilot and Google Gemini.

- BHASVIC recognises that AI has multiple uses to help students learn but may also have the potential to be used to harm or bully others. For example, in the form of 'deep fakes', where AI is used to create images, and audio or video hoaxes that look real. This includes deep fake pornography; abusive pornographic content created using AI to include someone's likeness.

- BHASVIC will investigate any use of AI to bully students in line with our Student Code of Conduct.

- Staff should be aware of the risks of using AI tools whilst they are still being developed and should assess risk where new AI tools are being used by the college. There is free gov.uk training available here: Using AI in education settings: support materials – GOV.UK

26. Data Protection

- The college's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The college will:

- Take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection.
- Use personal data only on secure password protected computers and other devices.
- Ensure that users are properly 'logged off' at the end of any session in which they are accessing personal data.
- Provide users with secure equipment/services to store or transfer data e.g. remote access, OneDrive, SharePoint, encryption, and secure password protected devices.
- Remove data in line with the college's GDPR (General Data Protection Regulation) Data Retention Policy.
- Ensure that all users are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead and that users understand the full requirements of the Data Protection Act 2018.
- Complete a Data Protection Impact Assessment (DPIA) and check the terms and conditions of sites/apps used for learning purposes to ensure that any personal data is being held securely.

27. Guidance and Legislation Informing this Policy:

- Keeping Children Safe in Education 2025 sets out specific responsibilities for governing bodies to ensure:
    - children and young people are taught about online safety
    - appropriate filters and appropriate monitoring systems are in place
    - online safety training for staff is integrated, aligned, and considered as part of the overarching safeguarding approach
- This policy is based on the DfE's statutory safeguarding guidance, KCSIE, and its advice for schools and colleges on:
    - Teaching online safety in schools
    - Preventing bullying - GOV.UK (www.gov.uk) and
    - Preventing bullying - GOV.UK (www.gov.uk)Searching, screening and confiscation
    - Prevent duty's statutory guidance regarding online safety and radicalisation (Home Office, 2023)

- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

- In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

28. Links to Legislation, Policies and Guidance

- **Anti-Phishing Working Group**
- **Appropriate Filtering and Monitoring: Safer Internet Centre**
- **Child Exploitation and Online Protection Command (CEOP)**
- **Childline**
- **Childnet**
- **Cyber Choices- National Crime Agency**
- **DofE Teachers' Standards**
- **Filtering and Monitoring standards for Schools and Colleges**
- **Internet Matters**
- **Internet Watch Foundation (IWF)**
- **Keeping Children Safe in Education 2025**
- **NSPCC**
- **Online Safety Act (2023)**
- **Prevent Duty Guidance England and Wales (2023)**
- **Professionals Online Safety Helpline**
- **Sharing nudes and semi-nudes: advice for education settings**
- **SWGfl: Report Harmful Content**
- **UK Safer Internet Centre**
- **Using AI in Education settings: Support materials**

Relevant Internal Documents and Policies:

Acceptable Use of IT Policy for Students

Bring your own Device (BYOD) Policy

Data Breach Notification Policy

Data Protection Policy

Data Retention Policy

Equality Diversity and Inclusivity Policy

Environment and Sustainability Policy

Freedom of Information Publication Scheme

Rights of Individuals Policy

Safeguarding and Child Protection Policy and Procedures

Addendum 2 to Safeguarding Policy - Preventing Extremism and Radicalisation
Safeguarding Policy

Privacy

SEND Policy

Student Behaviour Policy

Student Code of Conduct - College Contract

Student Voice Strategy

Whistleblowing Policy and Procedures

Guidance on SharePoint:

- Online Safety guidance for students and staff
- Digital Guidance for Students
- BHASVIC DigiLearn platform for staff