# Online Safety Policy

This policy applies to all members of Bath Academy community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Bath Academy aims to have robust processes in place to ensure the e-safety of students, staff and volunteers, deliver an effective approach to online safety and establish mechanisms to identify intervene and escalate an incident.
This policy is made available to staff at induction and through normal communication channels (school network, MS Teams: Safeguarding Team, published on the school website.

## Legislation and guidance

This policy is based on the DfE's statutory safeguarding guidance, Keeping Children Safe in Education 2024, and its advice for colleges on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.
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 cyber-bullying.

## Roles and responsibilities

This policy is applied and updated annually and its implementation is not the sole responsibility of any single person

The **Board of Directors** has overall responsibility for monitoring this policy including overall strategic responsibility for filtering and monitoring, as well as and holding the Principal to account for its effective implementation. They will attend regular meetings to discuss online safety, and monitor online safety logs as provided by the DSL. The Directors who oversee online safety are Mr. David Game and Mr. Mansour Kaveh.

The **Principal** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the college. The Principal also acts on reports and concerns.

The **Senior Management Team (SMT)** are also responsible for:

- Buying-in the filtering and monitoring system the college uses
- Documenting what is blocked or allowed, and why; the system must block harmful and inappropriate content, but should not unreasonably impact teaching and learning or school administration or restrict students from learning how to assess and manage risk themselves.
- Reviewing the effectiveness of our provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded
- Overseeing reports
- Making sure staff:
  - o Understand their role
  - o Are trained appropriately
  - o Follow policies, processes and procedures

The **Designated Safeguarding Lead** takes responsibility for online safety in college, in particular:
- Reviews filtering and monitoring reports
- Acts on safeguarding concerns
- Supports the Principal and SMT in ensuring staff implement this policy consistently throughout the college
- Working with staff, as necessary, to address any online safety issues or incidents
- Ensuring that online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that incidents of cyber-bullying are logged and dealt with in line with the college Behaviour Policy
- Delivering staff training on online safety

- Supporting and encouraging parents and carers to do what they can to keep their children safe online
- Supporting and encouraging students to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the Board of Directors

**ICT Support**: Himasou Makwana and the onsite ICT Officer are responsible for putting in place filtering and monitoring systems, which are updated regularly and keep students safe from inappropriate content and contact online while at college. Provide filtering and monitoring reports. He will ensure the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

**Curriculum Lead** Liam Hocking, Vice Principal works with Safeguarding Team to develop a planned and coordinated online safety education programme.

This will be provided through:
- PHSE and SRE (relationships and sex education) programmes
- Student development programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

**All staff** are responsible for maintaining an understanding of this policy, implementing this policy consistently and agreeing and adhering to the terms on acceptable use of the college's ICT systems and the internet.

**Parents** are expected to notify a member of staff or the Principal of any concerns or queries regarding this policy and ensure their child has read, understood and agreed to the terms on acceptable use of the college's ICT system.

**Visitors** and members of the community who use the college's ICT systems or internet will be made aware of this policy and expected to read and follow it. They will be expected to agree to the terms on acceptable use.
Current members of community:
Katerine Mallia – Todoelmundo
Vicky McDonald -Career Advice

### Educating students and parents about online safety
Students will be taught online safety as part of the curriculum and PSHE/RSE lessons. The college will use personal tutor meetings to raise awareness of the dangers that can be encountered online and may invite in speakers. The college will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

### Cyber-bullying
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. Further details of how the college deals with all forms of bullying including cyberbullying can be found in the Anti-Bullying Policy and Behaviour Policy. "How to report" Posters are displayed in the Staff room, Common student areas and Boarding House. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate and Student personal development programme.

### Acceptable use of the internet in college
Students, parents, staff, volunteers and directors must sign an agreement regarding the acceptable use of the college's ICT systems and the internet. Visitors will be expected to read and agree to the college's terms on acceptable use if relevant. Use of the college's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. The college will monitor the websites visited to ensure they comply with the above.

### Students using mobile devices in college
Any use of mobile devices in college by students must be in line with the acceptable use agreement. Any breach of the policy may trigger disciplinary action in line with the college Behaviour Policy. This applies to all devices with the capacity to connect to the internet and transfer data. This includes internet-connected toys, tablets, smart TVs and watches, phones, laptops and computers. All personal devices must connect to the internet using the Bath Academy WiFi.

**Staff using work devices outside college**
Staff members using a work device outside college must not install any unauthorised software on the device or use the device in a way which would violate the college's terms of acceptable use. Devices must be secure and password protected, and staff must not share their password with others. USB devices containing data must be encrypted.

**How the college will respond to issues of misuse**
Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the college's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The college will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**Training**
New staff members will receive training during induction on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. Staff members will receive refresher training at least once each academic year, as well as relevant updates as required. The DSL and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. Volunteers will receive appropriate training and updates, if applicable.

**Monitoring arrangements**
The DSL logs behaviour and safeguarding issues related to online safety on ISAMS from which an incident report log can be produced.

This policy is supplemented by a series of related acceptable use agreements, Appendix 1- 4.

This policy will be reviewed annually by the Designated Safeguarding Lead.

*Reviewed: November 2024*

*Next Review: November 2025*

*Responsible Officer: Natalia Knott*

## Social Media

### Expectations

• The expectations regarding safe and responsible use of social media applies to all members of Bath Academy.

• The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

• All members of Bath Academy are expected to engage in social media in a positive, safe and responsible manner.

All members of Bath Academy are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or that could damage the reputation of the college or individual within it.

• Bath Academy will control student and staff access to social media whilst using Bath Academy provided devices and systems on site.  Inappropriate or excessive use of social media during Bath Academy working hours or whilst using Bath Academy devices may result in disciplinary or legal action and/or removal of internet facilities.

• Concerns regarding the online conduct of any member of Bath Academy community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

### Staff Personal Use of Social Media

• The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

• Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct/ Staff behaviour policy as part of Acceptable Use Policy.

*Reputation*

• All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.

 Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in

their professional abilities.

• All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

    o Setting the privacy levels of their personal sites.

    o Being aware of location sharing services.

    o Opting out of public listings on social networking sites.

    o Logging out of accounts after use.

    o Keeping passwords safe and confidential and using two factor authentication wherever

    possible.

o Ensuring staff do not represent their personal views as that of the setting.

• Members of staff are encouraged not to identify themselves as employees of Bath Academy on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.

• All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.

• Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

• Members of staff will notify the Senior Management Team immediately if they consider that any content shared on social media sites conflicts with their role.

*Communicating with students and parents and carers*

• Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.)

Staff should not request or respond to any personal information from children. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

• Staff should not give out any personal contact details.

• On Bath Academy trips, staff should have a college mobile phone rather than having to rely on their own device.

• Staff should not accept friend requests from pupils. If a member of staff feels that this is necessary, they should first seek guidance from the DSL or a senior leader. If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.

• Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Principal (see *Staff Behaviour Policy/ Code of Conduct for further information*)

• Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Principal.

• Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputies).

**Students' Personal Use of Social Media**

• Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.

• We are aware that many popular social media sites state that they are not for children under the age of 13, (or 16 for WhatsApp), therefore we will not create accounts specifically for students under this age.

• Any concerns regarding students use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.

• Students will be advised:

    o To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

    o To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

    o Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

    o To use safe passwords and two factor authentication where possible.

    o To use social media sites which are appropriate for their age and abilities.

    o How to block and report unwanted communications.

    o How to report concerns both within the setting and externally.

    o To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

## Official Use of Social Media

Bath Academy official social media channels are a X account, Facebook page, Instagram, LinkedIn, Youtube.

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the Principal.
- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff use setting provided email addresses to register for and manage any official social media channels.
- Official social media sites are suitably protected and linked to our website.
- Public communications on behalf of Bath Academy will, where appropriate and possible, be read and agreed by at least one other colleague, Sam Hollingshead or Violet Dahl.
- Official social media use will be conducted in line with existing policies, including: antibullying, image/camera use, data protection, confidentiality and child protection.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

    Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

    Any official social media activity involving students will be moderated if possible.

    Parents and carers of students Under 18 will be informed of any official social media use with students; written parental consent will be obtained, as required.

    We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

*Staff expectations*

• If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

    o Sign our Acceptable use of ICT and Internet policy agreement.

o Always be professional and aware they are an ambassador for the setting.

o Disclose their official role but make it clear that they do not necessarily speak on behalf of Bath Academy.

o Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.

o Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.

o Ensure that they have appropriate consent from both pupils and parents before sharing images on the official social media channel.

o Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.

o Not engage with any direct or private messaging with current, or past, students, parents and carers.

o Inform their line manager, the DSL (or deputies) and/or the Principal of any concerns, such as criticism, inappropriate content or contact from students.

**Appendix I**

**Acceptable use of ICT and the Internet**
This agreement aims to keep all student's safe online when they join a course at Bath Academy.
Digital technology is constantly changing, and Bath Academy must play a key role in promoting internet safety to all students and parents. Bath Academy have online safety measures (e.g. filters, passwords, monitoring of online activity, monitoring of Geolocations etc) in place to help protect students in college and whilst using online platforms.
The online platforms Bath Academy are currently using, and which students may be asked to sign up for as part of their course, are;

- Zoom
- Microsoft Teams & Microsoft 36
- Let's Learn English – E-Learning
- Kahoot
- Seneca Learning
- Exampro
- Quizlet
- MorrisBy
- Cat4

We expect all students, regardless of age, to be responsible online, use the internet legally and follow the rules below;

- I will be responsible and careful in my online behaviour whilst part of a course at Bath Academy.  I will not do anything that might risk;
    - my own safety
    - the safety of other users (students, staff, Accommodation providers) connected to the college
    - the safety and security of the college's or other users' systems.
- I understand Bath Academy will monitor my online activity whilst in College, or attending classes online
- I will not share my username or password, or use another person's username or password
- I will not share details or passwords of online class meetings or share information within the classes other than with Bath Academy staff
- I will be aware of 'stranger danger' online and not share personal information (e.g. contact details or images) about myself or others online if I do not know them.
- I will immediately report to my teacher, a staff member or my accommodation host, any unpleasant or inappropriate material or messages that make me feel upset or unhappy through online platforms.
- I will only use my personal devices (mobile phones, iPads, Laptops, USB devices, smart watches etc) and college devices and I will follow this agreement when using Bath Academy equipment and/or my own equipment (e.g. phones / cameras / all other technology equipment), at all times during the course.
- I will not create, access (download or upload), share or store any illegal or inappropriate material, using my own or the college's equipment while on the course at Bath Academy. Illegal and inappropriate online materials include:
    - gambling, pornography, age-rated games/films, websites or games showing violence, any sort of extremism or being unkind to others (intolerance) based on race, religion, disability etc., sending or receiving words or pictures about sex, accessing and not paying for music and films that are protected or sending anything unpleasant or nasty.
- I will not install or store any programmes on college or other users' equipment that will alter or affect that equipment.
- When using personal devices in the college, I shall connect to the internet only via the Bath Academy WiFi.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will act as I want others to act towards me during my time online
- I will not access, copy, remove or alter other people's or the college's online materials or settings without their permission
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work
- I will be polite when I communicate with others online.  I will not use unkind, angry or bad language in texts, emails or any other online messages.
- I will not take, send or share on social media, pictures of anyone without their permission

- I will not meet anyone in real life who I have met online unless I have a member of Bath Academy staff or a Homestay Provider with me
- I will not ask my teacher or any adult from Bath Academy to be friend on Facebook, Instagram, Twitter or another social networking website.
- I understand that I have broken the Bath Academy rules if my online behaviour does not follow this Agreement and that I can be disciplined and given a warning. If I subsequently break the rules I understand I may be dismissed from lessons. If it is serious (e.g. breaking UK law) I could be removed from the College or I will be asked to leave the course (if Online).

This Agreement includes my time as a student of Bath Academy both in college and online, time away from the college (during holiday periods) and for the duration of the course, for my behaviour to other members of the college community.

<u>Further Information for Students and Parents</u>
Students, under the age of 18, that are taught one-to-one should have a parent supervising them during their lessons online. All one-to-one lessons will also be recorded by the teacher.
All online lessons are open to members of Bath Academy Senior Management Team to join at any time.

Any concerns that a student or parent have should be sent to Bath Academy Staff or to info@bathacademy.co.uk

We invite students to sign up for the online platforms. More information, for students and parents, of platforms in use at the college can be found here;
- Zoom - https://www.net-aware.org.uk/networks/zoom/
- Let's Learn English – E-Learning - https://letslearnenglish.com/faq/#faq33
- Microsoft Teams - https://support.microsoft.com/en-ie/office/distance-learning-with-office-365-guidance-for-parents-and-guardians-89d514f9-bf5e-4374-a731-a75d38ddd588
- Microsoft 365 - https://www.microsoft.com/en-ww/microsoft-365/what-is-microsoft-365
- Kahoot - https://kahoot.com/what-is-kahoot/
- Seneca Learning - https://senecalearning.com/en-GB/
- Exampro - https://www.exampro.co.uk/
- MorrisBy - https://www.morrisby.com/
- Cat4 - https://www.gl-assessment.co.uk/assessments/cat4/

Further information about Bath Academy's online safety measures can be found at:
https://www.bathacademy.co.uk/about-us/information-for-parents-students/e-safety-agreement/

Additional information on staying safe online can be found at:
- Safer Internet - https://saferinternet.org.uk/
- British Council - https://learnenglishteens.britishcouncil.org/uk-now/video-uk/online-safety-tips
- South West grid for Learning: https://swgfl.org.uk/online-safety/what-is-online-safety/

**Boarding Pupils**
Boarding pupils will be permitted internet access for their own devices. In addition to the normal filtering and logging on the system, some social media sites and apps are restricted due to their own recommended minimum age limits. Anyone using a personal device in the boarding house must connect to the internet via the college WiFi. If parents provide an alternative unfiltered internet connection (4G/5G) on phones or tablets, then they take full responsibility for the use and potential misuse of it by their child.

**Rules for the use of personal devices within college**
If students/Staff have been given permission to bring their own mobile devices to use in college, the rules for the use of these devices during the college day and in the boarding house (if applicable) are laid down below and must be adhered to.
- Students/Staff bringing a mobile device to college are to ensure the power supply is safe to use at all times.
- The owner of the mobile device is responsible for the actions of any other user who they permit to use it.
- Pornographic, indecent or images likely to offend others are not to be shown or saved on a mobile device.
- The wifi network must be used within college and boarding house and details of how to connect will be provided to all students during the first week of term.
- All Windows mobile devices are to have anti-virus software installed and kept up-to-date.
- The college will not provide any software for personal mobile devices.
- Users are responsible for ensuring that any important work is backed up regularly.
- Users are to allow access to files and folders on the device to any member of SMT if requested.

- The user is responsible for maintaining the device.
- The college accepts no responsibility for the security of the mobile device at any time.
- The use of mobile devices in college is subject to a separate policy and rules.
- Power leads are not to be trailed across any walking space.

**Appendix 2**

**Acceptable use of ICT and the internet**

**Student**

As a college user of the Internet, I agree to comply with the college rules on its use. I will use the Internet Access provided by the college in a responsible way, and observe all the restrictions explained to me by the college.
I also undertake to abide by college rules concerning the acceptable use of ICT resources, and respect the work and privacy of other students and staff.

If I use a personal mobile device within college, I agree to abide to the rules for the use of personal mobile devices and to provide any details requested and permit access to all files on it, if required.

Student Name _____ Student Signature _____Date: ___/___/___

**Parent**

As the parent or legal guardian of the student signing above, I grant permission for my son/daughter to use electronic mail and the Internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

I agree that should my son/daughter bring into college a personal mobile device that it remains the responsibility of the owner, and that any misuse may result in permission to use the mobile device being withdrawn.

Parent Name _____ Parent Signature _____Date: ___/___/___

I understand this Agreement and I know how important it is to not break these rules and the importance of acting safely and legally online. I accept that this Agreement is part of the Bath Academy Student Behaviour Policy.

Name:                          Signed:                          Date:

For Students under the age of 18

I understand this Agreement and have helped my child understand his/her responsibilities and the importance of acting safely and legally online. I accept that this Agreement is part of the Bath Academy Student Behaviour Policy.

Name:                          Signed:                          Date:

**Acceptable use of ICT and the Internet: All Staff (and Volunteers) Policy and Agreement Template**

*Please complete and return this form to the DSL*
As a user of the college computer systems, I agree to comply with the colleges Acceptable Usage Policy (AUP). I will use the computers, email and Internet provided by the college in a responsible way, and observe the restrictions explained to me.

## Bath Academy Policy

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

### This acceptable use policy is intended to ensure:
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The college will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

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

For my professional and personal safety:
- I understand that Bath Academy will monitor my use of the college digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the college digital technology systems are primarily intended for educational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Bath Academy systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Bath Academy policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in Bath Academy in accordance with the college policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (e.g. mobile phones, smart watches) in the college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment. I will also follow any additional rules set by the Bath Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on Bath Academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed by ICT Support person.
- I will not disable or cause any damage to college equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by college policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use policy applies not only to my work and use of Bath Academy digital technology equipment in school, but also applies to my use of Bath Academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Bath Academy.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name:     .................................................................

Signed:     .................................................................

Date:     .................................................................

**Acceptable use of ICT and the Internet: Guests**

*Please complete and return this form to the ICT Systems Manager.*

As a user of the college computer systems, I agree to comply with the colleges Acceptable Usage Policy (AUP). I will use the computers, email and Internet provided by the college in a responsible way, and observe all the restrictions explained to me.

I undertake to use the college ICT resources appropriately and will respect the privacy of other staff and students.

When using the colleges system I will ensure I do not compromise the security policies in place, particularly when connected to the network, and will not unauthorized persons to use my usernames or passwords at any time.

I understand that the ICT staff have unrestricted access to all areas of the network and that any laptop or portable storage device may be requested for inspection by ICT staff at any time and I must provide all necessary details on demand.

Name (Please Print Clearly) _____

Signature_____

Date: ___/___/___

**Appendix 3**

**Bath Academy College ICT use guidelines for parents**
Every attempt should be made for staff, parents and students to work together so that use of the internet is as safe as possible. All equipment and other users should be treated with respect and the facilities should be used in a way that does not disrupt its use by others.

This means that:
- users should take responsibility for their personal access facilities. They should not allow others access to their user IDs or email accounts and all passwords should be kept private and changed regularly
- no attempt should be made to bypass security or gain access to another user's account
- email addresses should only be passed to trusted individuals
- any email from unknown sources should be deleted immediately
- users should be made aware that inappropriate e-mail sent by them may be recorded and may be traced back to them
- any person who believes that attempts have been made to make unacceptable use of the internet should report the matter immediately to a member of staff
- any person who discovers any materials they consider may be offensive or inappropriate should report the matter immediately to a member of staff
- any material published on the Web or through other electronic means should not contain any offensive material and should be checked by a member of staff before being made publicly available
- users should not use their home address or phone number or those of other students or when on the network
- users should be aware that internet access is monitored and that every site they attempt to visit is recorded and may be traced back to them
- the college reserves the right to restrict or remove access in the event of any user misusing network and communication facilities.
- As well as these, a number of aspects are under the strict control of the classroom teacher.
- The use of chat and newsgroups is restricted. Any use of these facilities should be in line with specific instructions issued by the class teacher.
- Saving or downloading materials is subject to guidance from the class teacher. Materials saved or downloaded from the internet must not infringe copyright.
- Students must ensure that any form of removable data is virus free before using it.

# Online safety training needs – self audit for staff

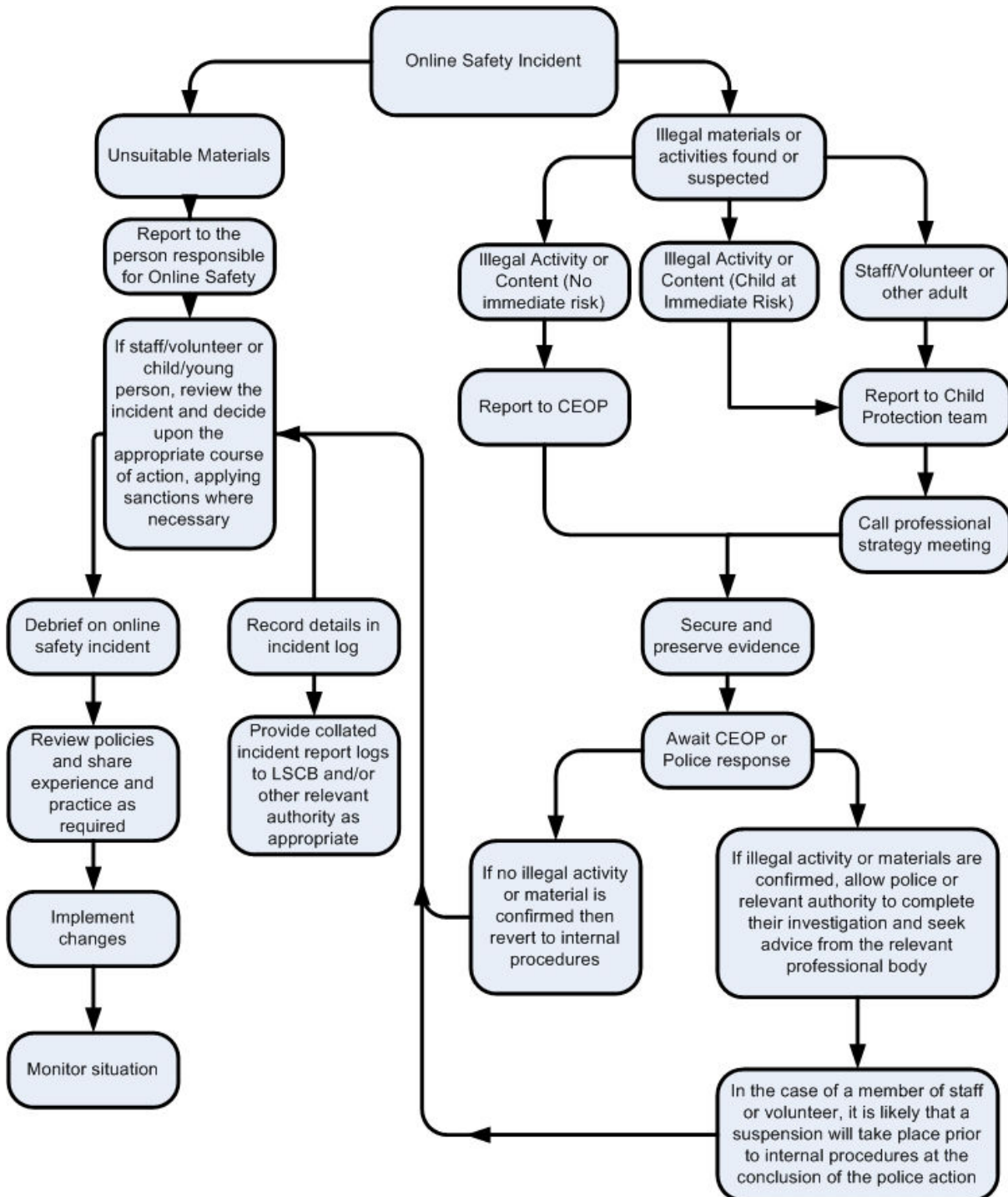| Online safety training needs audit | |
|---|---|
| Name of staff member/volunteer: | Date: |
| Do you know the name of the person who has lead responsibility for online safety in college? | |
| Do you know what you must do if a student approaches you with a concern or issue? | |
| Are you familiar with the college's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the college's acceptable use agreement for students and parents? | |
| Do you regularly change your password for accessing the college's ICT systems? | |
| Are you familiar with the college's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? Please record them here. | |

**Appendix 5**

## 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.

**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          Illegal Activity or   Illegal Activity or   Staff/Volunteer or
      for Online Safety           Content (No           Content (Child at     other adult
                                   immediate risk)       Immediate Risk)

      If staff/volunteer or
      child/young
      person, review the          Report to CEOP                              Report to Child
      incident and decide                                                     Protection team
      upon the
      appropriate course
      of action, applying
      sanctions where                                                         Call professional
      necessary                                                               strategy meeting

   Debrief on online      Record details in                 Secure and
   safety incident        incident log                   preserve evidence

   Review policies        Provide collated                Await CEOP or
   and share              incident report logs            Police response
   experience and         to LSCB and/or
   practice as            other relevant
   required               authority as          If no illegal activity   If illegal activity or materials are
                          appropriate           or material is           confirmed, allow police or
                                                 confirmed then           relevant authority to complete
   Implement                                     revert to internal       their investigation and seek
   changes                                       procedures               advice from the relevant
                                                                          professional body

   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
```

**Appendix 6**

## Reporting Log

| Incident | Action Taken | | Incident Reported By | Signature |
| --- | --- | --- | --- | --- |
| | What? | By Whom? | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |