Braunton Academy

Online Safety Policy

February 2026

If you require help in the interpretation of this policy, contact the DPO, Gary Brock

Scope of the Policy

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE) and other statutory documents; it is designed to sit alongside the Academy's Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow Braunton Academy's safeguarding and child protection procedures.

This policy applies to all members of Braunton Academy community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of Braunton Academy's digital technology systems, both in and out of Braunton Academy.

Our students are growing up in an increasingly complex world, living their lives seamlessly on and off-line. This presents many positive and exciting opportunities but also challenges and risks.

The use of the latest technology is actively encouraged at Braunton Academy but with this comes a responsibility to protect both students and the academy from abuse of the system.

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

Braunton Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of academy.

Roles and Responsibilities

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

Trustees

Trustees are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Trustee within the remit of Safeguarding Trustee.
The role of the Online Safety Trustee will include:

- regular meetings with the Designated Safeguarding Lead;
- regular monitoring of the safeguarding incident logs;
- reporting to relevant Trustees meeting.
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)

- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually
- reporting to relevant *Trustees group/meeting*
- Receiving (at least) basic cyber-security training to enable the Trustees to check that the academy meets the DfE Cyber-Security Standards

Principal and Lead Teachers

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the academy community and has delegated the role of Online Safety Lead to the Designated Safeguarding Officer.
- The Principal and Lead Teachers should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Principal is responsible for ensuring that suitable training is made available to relevant staff to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in academy who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles. This is currently delegated to Integy with any breaches being reported to the Principal.

Online Safety Lead

The Vice-Principal Inclusion (DSL) is the Online Safety Lead. In the capacity as Online Safety Lead:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy online safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- provides training and advice for staff;
- stay up to date with the latest trends in online safety
- ensure that online safety education is embedded across the curriculum and beyond, in wider academy life
- promote an awareness and commitment to online safety throughout Braunton Academy community, with a strong focus on parents, who are often appreciative of Braunton Academy support in this area, but also including hard-to-reach parents
- liaises with the Local Authority;
- liaises with Braunton Academy technical staff (outsourced to Integy)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- meets regularly with the Safeguarding Trustee to discuss current issues and review incident logs.

Network Manager (Integy)

Those with technical responsibilities are responsible for ensuring:

- that Braunton Academy's technical infrastructure is secure and is not open to misuse or malicious attack;
- that Braunton Academy meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Vice Principal Inclusion for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in Braunton Academy's policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Braunton Academy Online Safety Policy and practices;
- they have read, understood and signed the staff acceptable use policy (AUP);
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Coordinator (OSC) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for Senior management team and those working directly with children, it is good practice for all staff to read all three sections).
- they report any suspected misuse or problem to the Principal or Lead Teachers for investigation/action/sanction;
- all digital communications with students/parents/carers should be on a professional level and only carried out using official Braunton Academy systems; (where staff use AI, they should only use academy-approved AI services for work purposes which have been evaluated to comply with organisational and oversight requirements)
- online safety issues are embedded in all aspects of the curriculum and other activities;
- students understand and follow the Online Safety Policy and Acceptable Use policies;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other academy activities (where allowed) and implement current policies regarding these devices. Braunton Academy is a Smart device free school for all students. Please refer to the Smartphone Free Policy for further guidance.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- model safe, responsible and professional behaviours in their own use of technology. This includes outside the academy hours and site, and on social media, in all aspects upholding the reputation of the academy and of the professional reputation of all staff.
- follow the remote learning guidelines and teacher protocols during any part or full Braunton Academy closure
- they adhere to the Academy's Technical Security guidance, regarding the use of devices, systems and passwords and understand basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of academy, to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in academy, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated. Please refer to the Academy's AI policy.

Designated Safeguarding Lead

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

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- online-bullying.

Students:

- are responsible for using Braunton Academy digital technology systems in accordance with the student acceptable use agreement;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras (they are banned at the school and on school trips, see the Smartphone policy). They should also know and understand policies on the taking/use of images and on online bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of academy and realise that Braunton Academy's online safety policy covers their actions out of academy, if related to their membership of the Academy.

Parents/carers

- Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Braunton Academy will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.
- Read and sign the parental acceptable use agreement, including remote learning protocols, read the student acceptable agreement and encourage their children to follow it.
- Parents/carers are mindful of social media expectations, and data protection not to share information, speculation and gossip about the academy, staff, other parents or students.
- Parents/carers will be encouraged to support Braunton Academy in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at academy events;
    - learning apps such as Sparx and Educake
    - their children's use of loaded devices for remote learning and/or access to learning apps for homework.

External Groups (including parent associations)

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within Braunton Academy
- support Braunton Academy in promoting online safety and data protection
- model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including Braunton Academy staff and Trustees, volunteers, contractors, students or other parents/carers.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of Braunton Academy 's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience.

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

- a planned online safety curriculum should be provided as part of Computing/PD/other lessons and should be regularly revisited;

- key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;
- students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
- students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Braunton Academy;
- staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;
- it is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Integy can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents/careers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- letters, newsletters, website;
- parents/carers evenings/sessions;
- high profile events/campaigns e.g. Safer Internet Day;
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (see appendix for further links/resources)

Good Advice and Practice for Parents

- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.

- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is important.

Education – The Wider Community

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

- providing family learning courses in use of new digital technologies, digital literacy and online safety;
- online safety messages targeted towards grandparents and other relatives as well as parents;
- Braunton Academy website will provide online safety information for the wider community;
- sharing their online safety expertise/good practice with other local schools;
- supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Braunton Academy Online Safety Policy and Acceptable Use agreements;
- online safety will be integral to ongoing safeguarding training;
- it is expected that some staff will identify online safety as a training need within the performance management process;
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions;
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Trustees

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

- Attendance at training provided by the Local Authority;
- Participation in Braunton Academy training/information sessions for staff or parents/carers.

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of academy life

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence

- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the academy and wider community, using officially sanctioned academy mechanisms.
- Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

Technical – infrastructure/equipment, filtering and monitoring

Under the direction of Braunton Academy, Integy will be responsible for ensuring that Braunton Academy's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Braunton Academy technical systems will be managed in ways that ensure that Braunton Academy meets recommended technical requirements;
- there will be regular reviews and audits of the safety and security of Braunton Academy technical systems;
- servers, wireless systems and cabling must be securely located and physical access restricted;
- all users will have clearly defined access rights to Braunton Academy technical systems and devices;
- all users will be provided with a username and secure password by Integy;
- the "master/administrator" passwords for Braunton Academy systems, used by the Network Manager (Integy) must also be available to the Principal/ and kept in a secure place (e.g. Braunton Academy safe);
- Integy is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes;
- internet filtering/monitoring should ensure that students are safe from terrorist and extremist material when accessing the internet;
- Braunton Academy has provided enhanced/differentiated user-level filtering;
- Integy regularly monitor and record the activity of users on Braunton Academy technical systems and users are made aware of this in the Acceptable Use Agreement;
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person;
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of Braunton Academy systems and data. These are tested regularly. Braunton Academy infrastructure and individual devices are protected by up-to-date virus software;
- an agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the academy systems;
- an agreed policy is in place regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on academy devices that may be used out of academy;
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on Braunton Academy devices. Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices are only permitted to staff and a minority of students which specific medical needs or SEND needs, e.g. student laptops (see Smartphone policy). Staff may have Braunton Academy owned/provided or personally owned devices and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising Braunton Academy 's wireless network. The device then has access to the wider internet, which may include cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in an Academy context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant Braunton Academy polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of Braunton Academy 's online safety education programme. Braunton Academy Acceptable Use Agreements for staff, students and parents/carers will consider the use of mobile technologies. The academy allows:

	Academy Devices			Personal Devices		
				Student owned	**Staff owned**	**Visitor owned**
Allowed in academy	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*N/A*	*No*	*No*
Internet only	*N/A*	*N/A*	*N/A*	*N/A*	*Yes*	*Yes*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Braunton Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- written permission from parents or carers will be obtained before photographs of students are published on the academy website/social media/local press;
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Braunton Academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students* in the digital/video images;
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Braunton Academy policies concerning the sharing, distribution and publication of those images;
- care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or Braunton Academy into disrepute;
- students must not take, use, share, publish or distribute images of others without their permission;

- photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- students' full names will not be used anywhere on a website or blog, particularly in association with photographs. Where exceptional individual achievement may warrant the naming of an individual (such as winning a national title representing Braunton Academy (and this information will be available publicly on other websites), then a student's full name may be justified, with additional consent from parents. (This could be via email and consent must be obtained each time this occurs)

Data Protection[FB1]

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

Braunton Academy must ensure that:

- it has a Data Protection Policy;
- it implements the data protection principles and can demonstrate that it does so through use of policies, notices and records;
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO);
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest;
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it;
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded;
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- it provides staff, parents and volunteers with information about how Braunton Academy looks after their data and what their rights are in a clear Privacy Notice;
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum);
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring-fenced from systems accessible in the classroom/to learners;
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed;
- it understands how to share data lawfully and safely with other relevant data controllers;
- it reports any **relevant** breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a procedure for reporting, logging, managing, investigating and learning from information risk incidents; All breaches including minor ones must be reported to Braunton Academy Principal and DPO (who will log the breach) and who together will consider if the breach reaches the threshold of reporting the breach to the ICO.
- it must have a Freedom of Information Policy which sets out how it will deal with FOI requests;
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected;
- device must be password protected;

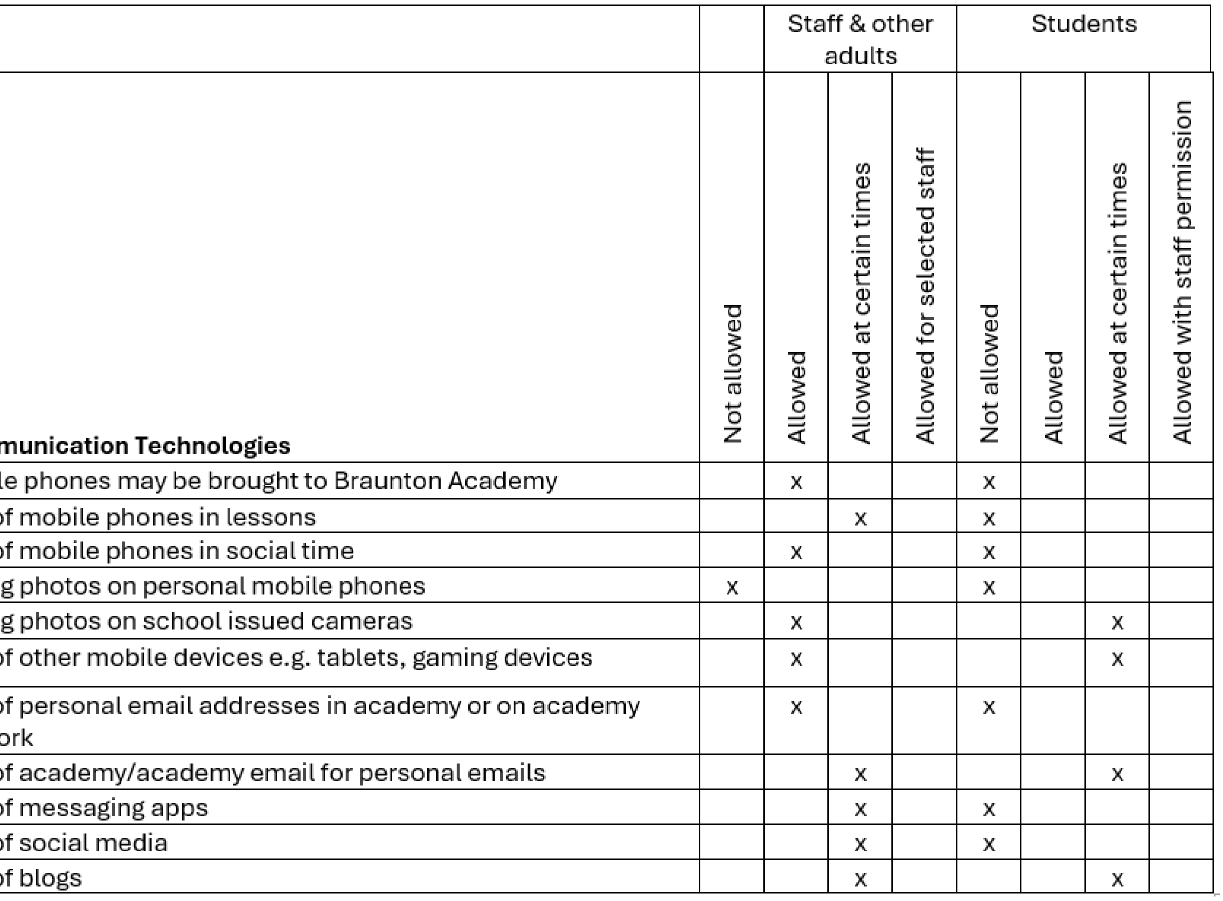
- device must be protected by up-to-date virus and malware checking software;
- data must be securely deleted from the device, in line with Braunton Academy policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- can recognise a possible breach, understand the need for urgency and know who to report it to within Braunton Academy;
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in Braunton Academy;
- where personal data is stored or transferred on mobile or other devices these must be encrypted and password protected;
- will not transfer any Braunton Academy personal data to personal devices except as in line with academy policy;
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly “logged off” at the end of any session in which they are using personal data.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how Braunton Academy currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:



		Staff & other adults			Students			
munication Technologies	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
le phones may be brought to Braunton Academy		x			x			
of mobile phones in lessons			x		x			
of mobile phones in social time		x			x			
g photos on personal mobile phones	x				x			
g photos on school issued cameras		x					x	
of other mobile devices e.g. tablets, gaming devices		x					x	
of personal email addresses in academy or on academy ork		x			x			
of academy/academy email for personal emails			x				x	
of messaging apps			x		x			
of social media			x		x			
of blogs			x				x	

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

- the official Braunton Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only Braunton Academy email service to communicate with others when in academy, or on Braunton Academy systems (e.g. by remote access);
- users must immediately report to the nominated person – in accordance with Braunton Academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
- any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Braunton Academy systems. Personal email addresses, text messaging or social media must not be used for these communications unless via an approved group, e.g., closed social media groups when students are on residential;
- students will be provided with individual Braunton Academy email addresses for educational use;
- students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;
- personal information should not be posted on Braunton Academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render Braunton Academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Braunton Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and Braunton Academy through:

- Smartphone free policy in school
- Collaboration with Smartphone Free Childhood to support understanding of the harms associated with use of smartphones and social media at a young age
- ensuring that personal information is not published
- training is provided including acceptable use; social media risks; checking of settings; data protection; information security, reporting issues;
- clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

Braunton Academy staff should ensure that:

- no reference should be made in social media to students, parents/carers or Braunton Academy staff;
- they do not engage in online discussion on personal matters relating to members of Braunton Academy community;
- personal opinions should not be attributed to Braunton Academy or Local Authority;
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

When official Braunton Academy social media accounts are established, there should be:

- a process for approval by senior leaders;
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
- a code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse;
- understanding of how incidents may be dealt with under Braunton Academy disciplinary procedures.

Personal Use:

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with Braunton Academy or impacts on Braunton Academy, it must be made clear that the member of staff is not communicating on behalf of Braunton Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy;
- personal communications which do not refer to or impact upon Braunton Academy are outside the scope of this policy;
- where excessive personal use of social media in academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken;
- Braunton Academy permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media:

- as part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Braunton Academy;
- Braunton Academy should effectively respond to social media comments made by others according to the following process:
    - ▪ All official social media sites are locked down to stop any member of the public commenting

- If you are made aware of a social media post which you feel is inappropriate about the Academy, a member of staff or student you should alert the DSL. **You must not respond on behalf of the school.**
- The DSL will liaise with the Principal to determine whether an official response or action needs to be taken on behalf of the Academy to protect the Academy or staff reputation or mange a safeguarding issue for students.

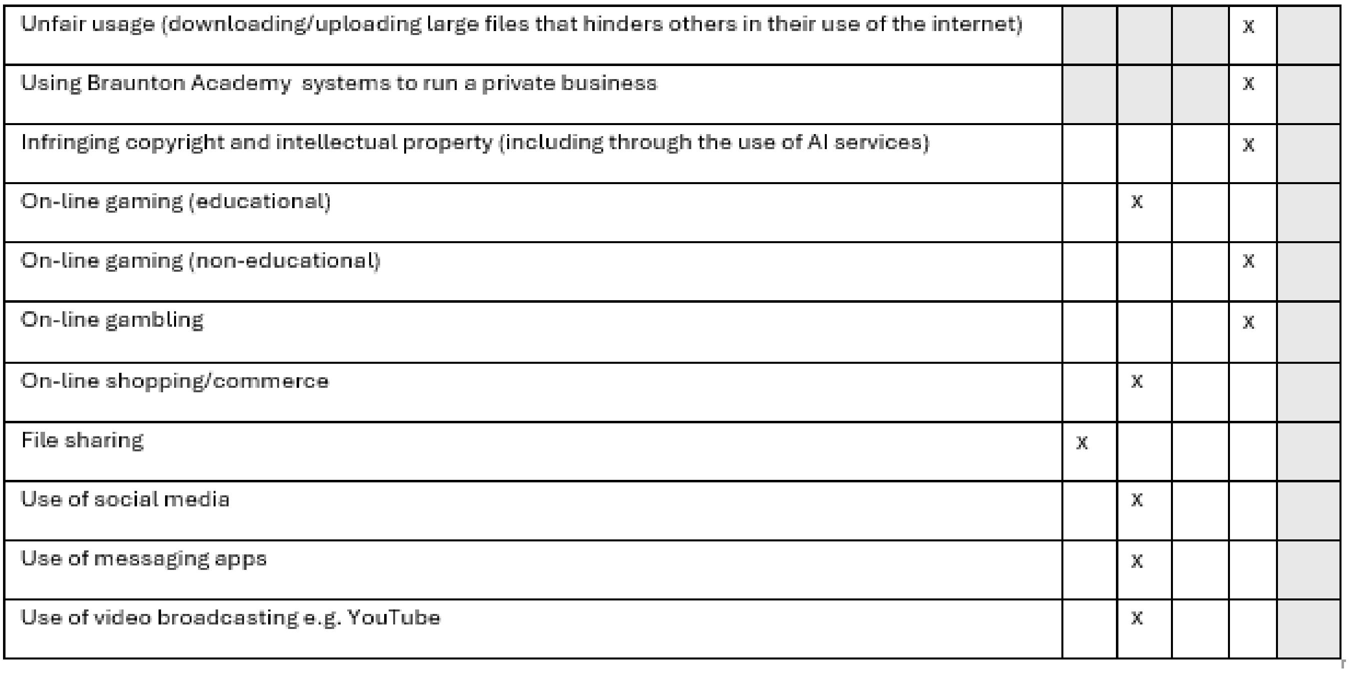
Braunton Academy 's use of social media for professional purposes will be checked regularly by the Principal to ensure compliance with Braunton Academy policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Braunton Academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					x
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					x
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					x
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					x
	Pornography				x	
	Promotion of any kind of discrimination				x	
	Threatening behaviour, including promotion of physical violence or mental harm				x	
	Promotion of extremism or terrorism					x
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of Braunton Academy or brings Braunton Academy into disrepute				x	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to academy networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Braunton Academy					x	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					x	



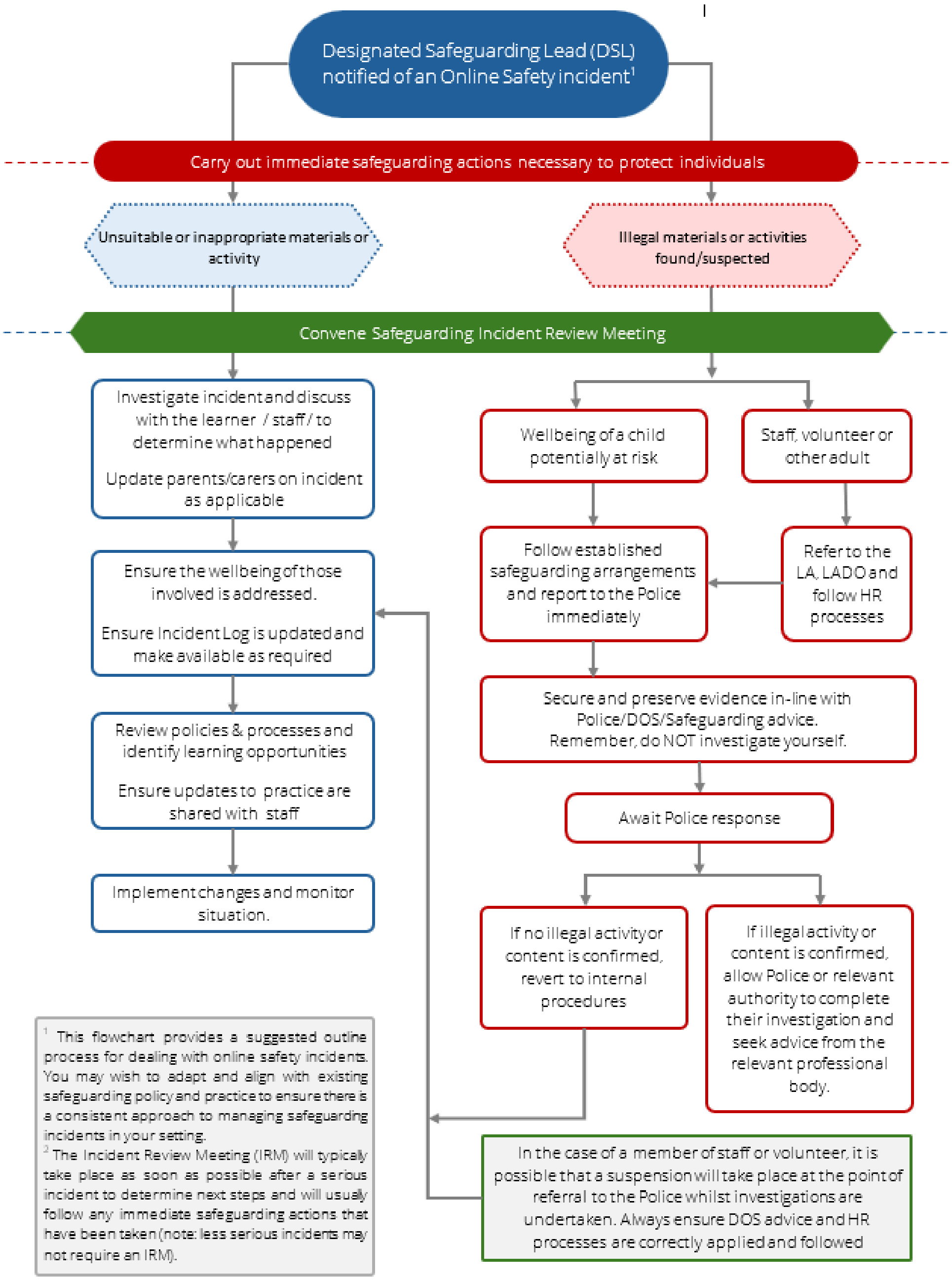
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				x	
Using Braunton Academy systems to run a private business				x	
Infringing copyright and intellectual property (including through the use of AI services)				x	
On-line gaming (educational)		x			
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping/commerce		x			
File sharing	x				
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. YouTube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police. [FB2]


Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]
Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Convene Safeguarding Incident Review Meeting
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Other Incidents

It is hoped that all members of Braunton Academy community will be responsible users of digital technologies, who understand and follow Braunton Academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below);

- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures;
    - Involvement by Local Authority;
    - Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

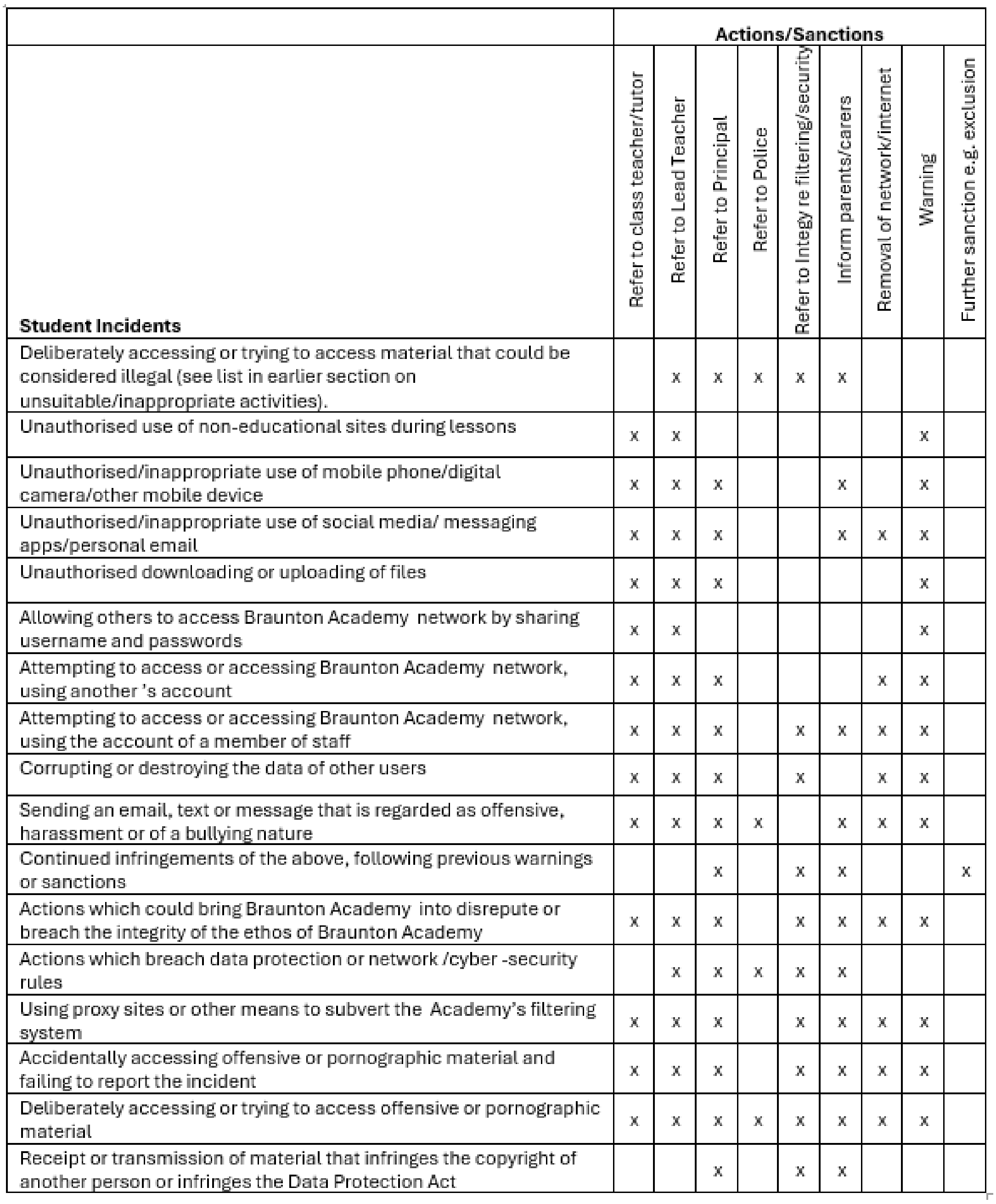
- incidents of 'grooming' behaviour;
- the sending of obscene materials to a child;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- promotion of terrorism or extremism;
- offences under the Computer Misuse Act (see User Actions chart above);
- other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

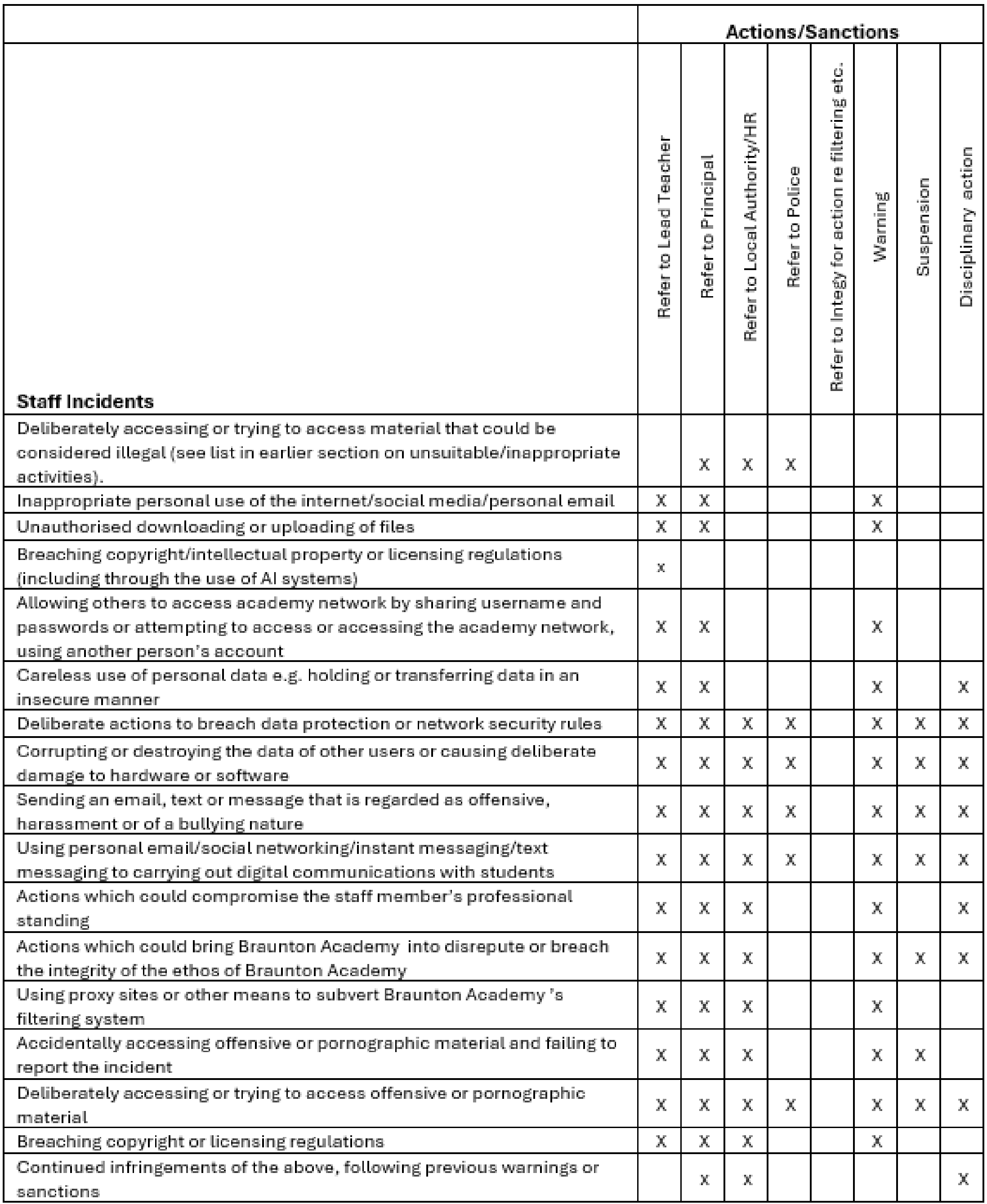
It is important that all the above steps are taken as they will provide an evidence trail for Braunton Academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI may miss.

Braunton Academy actions & sanctions
It is more likely that Braunton Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of Braunton Academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:



	Actions/Sanctions								
Student Incidents	Refer to class teacher/tutor	Refer to Lead Teacher	Refer to Principal	Refer to Police	Refer to Integy re filtering/security	Inform parents/carers	Removal of network/internet	Warning	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		x	x	x	x	x			
Unauthorised use of non-educational sites during lessons	x	x						x	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x	x	x			x		x	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	x	x	x			x	x	x	
Unauthorised downloading or uploading of files	x	x	x					x	
Allowing others to access Braunton Academy network by sharing username and passwords	x	x						x	
Attempting to access or accessing Braunton Academy network, using another 's account	x	x	x				x	x	
Attempting to access or accessing Braunton Academy network, using the account of a member of staff	x	x	x		x	x	x	x	
Corrupting or destroying the data of other users	x	x	x		x		x	x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x		x	x	x	
Continued infringements of the above, following previous warnings or sanctions			x		x	x			x
Actions which could bring Braunton Academy into disrepute or breach the integrity of the ethos of Braunton Academy	x	x	x		x	x	x	x	
Actions which breach data protection or network /cyber -security rules		x	x	x	x	x			
Using proxy sites or other means to subvert the Academy's filtering system	x	x	x		x	x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x	x	x	x	
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x		x	x			



	Actions/Sanctions							
Staff Incidents	Refer to Lead Teacher	Refer to Principal	Refer to Local Authority/HR	Refer to Police	Refer to Integy for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Breaching copyright/intellectual property or licensing regulations (including through the use of AI systems)	x							
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	X	X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		X
Deliberate actions to breach data protection or network security rules	X	X	X	X		X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students	X	X	X	X		X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X		X
Actions which could bring Braunton Academy into disrepute or breach the integrity of the ethos of Braunton Academy	X	X	X			X	X	X
Using proxy sites or other means to subvert Braunton Academy 's filtering system	X	X	X			X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X	X
Breaching copyright or licensing regulations	X	X	X			X		
Continued infringements of the above, following previous warnings or sanctions		x	x					X

The use of Artificial Intelligence (AI) systems in Academy

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The academy acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR.
- We will provide relevant training for staff and Trustees in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The academy recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the academy.
- Only those AI technologies approved by the academy may be used. Staff should always use academy-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The academy will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The academy will audit all AI systems in use and assess their potential impact on staff, learners and the Academy's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The academy will support parents and carers in their understanding of the use of AI in the academy (this could be through an "AI in our academy guide")[FB3]
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents. [FB4][EW5]
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Appendix

Student Acceptable Use Agreement[FB6]

Braunton Academy Policy

Digital technologies have become integral to the lives of children and young people, both within Braunton Academy and outside the academy. These 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. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that Braunton Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use Braunton 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.

For my own personal safety:

- I understand that Braunton Academy will monitor my use of the systems, devices and digital communications;
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.);
- I will not arrange to meet people off-line that I have communicated with on-line unless under the guidance and supervision of a trusted adult;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Braunton Academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission;
- 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 use Braunton Academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so;
- I will act as I expect others to act toward me;
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will not take or distribute images of anyone without their permission.

I recognise that Braunton Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Braunton Academy:

- I will not use my own personal devices;

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software; however, this may have happened;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any academy device, nor will I try to alter computer settings;
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should 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 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 that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of academy:

- I understand that Braunton Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of academy and where they involve my membership of Braunton Academy community (examples would be online-bullying, use of images or personal information);
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the academy network/internet, contact with parents and in the event of illegal activities involvement of the police and possible exclusion.

Students will be made aware of this agreement through computing and PD lessons. A copy of the agreement will be displayed in and/or adjacent to lap top trolleys and within classrooms.[FB7]

💻 Braunton Academy – Student Acceptable Use Agreement

This agreement explains how you should use computers, the internet, and devices at school. It keeps **you safe** and makes sure **everyone can learn**.

👤 My Safety Online

- 🔍 **School checks use** → Teachers can see what I do online.
- 🔑 **Keep passwords secret** → Don't share or write them down.

- 🚫 **Stranger danger** → Don't talk to strangers online.
- 🛑 **No personal info** → Don't share name, address, phone, or photos.
- 👥 **No secret meetings** → Don't meet online friends without an adult.
- ⚠️ **Report problems** → Tell a teacher if something online worries you.

🤝 Respecting Others

- 📚 **Use for learning** → School computers are mainly for schoolwork.
- 📥 **No big downloads** → Don't block the internet with huge files.
- 🎮 **No games/shopping** → Unless a teacher says it's okay.
- 📝 **Respect work** → Don't change or copy other people's files.
- 💬 **Be kind** → Use polite words online.
- 📸 **Ask first** → Don't take or share photos of others without permission.

🔒 Keeping School Systems Safe

- 📵 **No personal devices** → Use school computers, not your own.
- 🚫 **No bad sites** → Don't try to see or share harmful or illegal stuff.
- 💻 **Report damage** → Tell staff if something is broken.
- 📧 **Be careful with emails** → Only open links/attachments from people you trust.
- ⚙️ **Don't change settings** → Don't install apps or change computers.
- 🌐 **Social media rules** → Only use when allowed by staff.

🌍 Using the Internet

- 📝 **Check permission** → Don't copy other people's work without asking.
- 🎵 **No illegal downloads** → Don't copy music or videos.
- ❓ **Think carefully** → Not everything online is true.

⚖️ My Responsibility

- 🏫 **In school and out** → Rules apply everywhere, not just at school.
- 🚫 **No bullying** → Don't use tech to upset others.
- ⚠️ **Consequences** → Breaking rules may mean losing computer access, parents being told, or police involvement.

📌 Remember

- This agreement will be taught in lessons.
- Copies will be shown near laptops and in classrooms.

☑ Student Promise

I agree to use Braunton Academy technology safely, kindly, and responsibly.

.

Parent/Carer Acceptable Use Agreement [FB8]

Digital technologies have become integral to the lives of children and young people, both within and outside the academy. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that academy/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people regarding their on-line behaviour.

Braunton Academy will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students/students to agree to be responsible users. A copy of the student acceptable use agreement is attached to this permission form, so that parents/carers will be aware of Braunton Academy expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of Braunton Academy in this important aspect of Braunton Academy 's work.

Permission Form

Parent/Carers Name:

Student Name:

As the parent/carer of the above student(s), I give permission for my son/daughter to have access to the internet and to ICT systems at academy.

I understand that the academy has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of academy.

I understand that Braunton Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that Braunton Academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that Braunton Academy will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform Braunton Academy if I have concerns over my child's online safety.

Signed:

Date:

Staff (and Volunteer) Acceptable Use Policy Agreement

Academy Policy

New technologies have become integral to the lives of children and young people today, both within and in their lives outside Braunton Academy. The internet and other digital information and communications technologies are powerful tools, which open 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 always have an entitlement to safe access to the internet and digital technologies.

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 Braunton Academy 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.

Braunton Academy will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students 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 Braunton 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 students 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 Braunton Academy will monitor my use of Braunton Academy 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, VLE etc.) out of the academy, and to the transfer of personal data (digital or paper based) out of the academy;
- I understand that Braunton Academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Braunton Academy;
- 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 Braunton 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 Braunton Academy 's 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 Braunton Academy website/VLE) 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 academy in accordance with Braunton Academy 's policies, e.g., closed Facebook groups;

- I will only communicate with students and parents/carers using official Braunton Academy systems (email) 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.

Braunton Academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Braunton Academy:

- When I use my mobile devices in academy, I will follow the rules set out in this agreement, in the same way as if I was using Braunton Academy equipment. I will also follow any additional rules set by Braunton 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;
- If my personal device(s) access Braunton Academy email and other Braunton Academy 'educational use' apps and software, I must enable suggested patches and software updates as these updates mostly fix security weaknesses and failure to update makes my personal device(s) vulnerable to malicious attacks which may compromise and put Braunton Academy at risk.
- I will not use personal email addresses on Braunton 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 Braunton Academy 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 in Braunton Academy policies;
- I will not disable or cause any damage to Braunton Academy equipment, or the equipment belonging to others;
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in Braunton Academy 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 student 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 Braunton Academy 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 internet in my professional capacity or for Braunton Academy 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 Braunton Academy:

- I understand that this acceptable use policy applies not only to my work and use of Braunton Academy digital technology equipment in academy, but also applies to my use of Braunton Academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Braunton 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 Trustees 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 Braunton Academy digital technology systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to Braunton Academy) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Braunton Academy

Staff & Volunteer Acceptable Use Policy (AUP) *Friendly Guide for Staff and Parents*

Why this policy matters

Digital technology is a big part of everyday life for our students, staff, and volunteers. At Braunton Academy, we use the internet, email, and other digital tools to support learning, creativity, and communication. With these opportunities come responsibilities: we must all use technology safely, respectfully, and responsibly.

This policy explains how staff and volunteers are expected to use Braunton Academy systems and devices. It helps protect:

- **Students** – by keeping them safe online
- **Staff and volunteers** – by reducing risks in everyday work
- **The Academy** – by keeping our systems secure and running smoothly

Key Principles

- Use technology responsibly and safely, both in and outside the Academy.
- Protect personal information and respect privacy.
- Always communicate professionally.
- Follow Academy rules when using personal devices for work.
- Report anything unsafe, inappropriate, or broken straight away.

What staff and volunteers agree to

Staying safe

- The Academy may monitor use of its systems.
- Rules apply whether you're on-site or working from home.
- Systems are mainly for education. Limited personal use is fine but must follow Academy rules.
- Keep your login details private. Never share passwords.

- Report anything harmful, illegal, or suspicious immediately.

Professional behaviour

- Be respectful in all online communication.
- Do not access or change other people's files without permission.
- Only take or share photos/videos with permission and follow Academy image policies.
- Use official Academy systems (e.g. email) to contact students or parents.
- Avoid online activity that could compromise your professional role.

Using devices

- Personal devices used for Academy work must have up-to-date security software.
- Install updates when prompted to keep devices secure.
- Do not use personal email accounts on Academy systems.
- Be cautious with email links and attachments – only open if trusted.
- Back up important data regularly.
- Never download or share illegal or harmful material.
- Do not try to bypass Academy security filters.
- Avoid large downloads/uploads that could slow down the network.
- Do not install software or change settings unless authorised.
- Keep paper records with personal data locked away; digital data must be encrypted if taken off-site.

Data protection

- Keep staff and student information confidential.
- Share personal data only when required by law or Academy policy.
- Report any damage, faults, or security concerns immediately.

Copyright and fair use

- Always credit original work.
- Do not copy or distribute copyrighted material (music, films, etc.) without permission.

Responsibilities beyond the Academy

- This agreement applies both inside and outside the Academy, and when using personal devices for Academy work.
- Breaching this policy may lead to disciplinary action, including warnings, suspension, referral to Trustees or the Local Authority, and in serious cases, police involvement.

Agreement

By signing below, you confirm that you understand and will follow Braunton Academy's Acceptable Use Policy.

Staff/Volunteer Name: ____________________________ **Signed:** ____________________________ **Date:** ____________________________

Acceptable Use Agreement for Community Users [FB9]

This acceptable use agreement is intended to ensure:

- that community users of Braunton Academy digital technologies will be responsible users and stay safe while using these systems and devices;
- that Braunton Academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use Braunton Academy systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into Braunton Academy:

- I understand that my use of Braunton Academy systems and devices will be monitored;
- I will not use a personal device that I have brought into academy for any activity that would be inappropriate in an academy setting;
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person;
- I will not access, copy, remove or otherwise alter any other user's files, without permission;
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured;
- I will not publish or share any information I have obtained whilst in the academy on any personal website, social networking site or through any other means, unless I have permission from Braunton Academy;
- I will not, without permission, 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 Braunton Academy device, nor will I try to alter computer settings, unless I have permission to do so;
- I will not disable or cause any damage to Braunton Academy equipment, or the equipment belonging to others;
- I will immediately report any damage or faults involving equipment or software; however, this may have happened;
- 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 if I fail to comply with this acceptable use agreement, Braunton Academy has the right to remove my access to Braunton Academy systems/devices.

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

Name:

Signed:

Date:

Record of reviewing devices/internet sites (responding to incidents of misuse)

Date:

Reason for investigation:

Details of first reviewing person
Name:
Position:
Signature:

Details of second reviewing person
Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

Web site(s) address/device	*Reason for concern*
Conclusion and Action proposed or taken	

Reporting Log

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Academy Technical Security Policy Template (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Braunton Academy will be responsible for ensuring that Braunton Academy infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access;
- A documented access control model is in place, clearly defining access rights to academy systems and devices. This is reviewed annually. All users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- no user should be able to access another's files (other than that allowed for monitoring purposes within Braunton Academy 's policies);
- access to personal data is securely controlled in line with Braunton Academy 's personal data policy;
- logs are maintained of access by users and of their actions while users of the system;
- there are effective guidance and training for users;
- there are regular reviews and audits of the safety and security of Braunton Academy computer systems;
- there is oversight from senior leaders, and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Integy, under the direction of the Principal.

Technical Security Policy Statements

Braunton Academy will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- Braunton Academy technical systems will be managed in ways that ensure that Braunton Academy meets recommended technical requirements;
- there will be regular reviews and audits of the safety and security of Braunton Academy technical systems;
- servers, wireless systems and cabling must be securely located and physical access restricted;
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of Braunton Academy systems and data;
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff employed by Integy;
- all users will have clearly defined access rights to Braunton Academy technical systems. Details of the access rights available to groups of users will be recorded by Integy. There is an agreed policy in place for temporary access.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- Integy is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- mobile device security and management procedures are in place;
- remote management tools are used by staff to control workstations and view users' activity;
- an appropriate system is in place for users to report any actual/potential technical incident to the Principal.
- Temporary access will be granted to enable access to the internet but not Braunton Academy intranet;
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on Braunton Academy devices that may be used out of academy (limited personal use that is in accordance with Braunton Academy general acceptable use policy);
- Braunton Academy infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc;
- personal data cannot be sent over the internet or taken off the academy/academy site unless safely encrypted or otherwise secured.

- All internal emails are encrypted and use of encryption systems such as egress are used to share personal and sensitive data to external agencies.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- multi-factor authentication is used for sensitive data or access outside of a trusted network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the academy will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias
-

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all Braunton Academy technical systems, including networks, devices, email and learning platform. Where sensitive data is in use more secure forms of authentication e.g. two factor authentication, should be used, eg CPOMS. Further guidance can be found from the National Cyber Security Centre and SWGfL "Why password security is important"

Policy Statements

These statements apply to all users:

- All Braunton Academy networks and systems will be protected by secure passwords;
- all users have clearly defined access rights to Braunton Academy technical systems and devices. Details of the access rights available to groups of users will be recorded by Integy and will be reviewed, at least annually, by the Principal;
- all users (adults and students) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- passwords must not be shared with anyone;
- all users will be provided with a username and password by Integy or a member of the SLT who will keep an up-to-date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack;
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of Braunton Academy;
- passwords must not include names or any other personal information about the user that might be known by others;
- passwords must be changed on first login to the system;
- passwords should not be set to expire if they comply with the above but should be unique to each service the user logs into.

Learner passwords:

- Records of learner usernames and passwords for students can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user;
- users will be required to change their password if it is compromised;
- students will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff

Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.

- An administrator account password for Braunton Academy systems should also be kept in a secure place e.g. Braunton Academy safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account;
- any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used;
- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password;
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by Integy or a member of the SLT. Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary, and the user should be forced to change their password on first login. The generated passwords should also be long and random;
- Staff requests for password changes should be authenticated by the operations manager to ensure that the new password can only be passed to the genuine user;
- In good practice, the account is "locked out" following six successive incorrect log-on attempts;
- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way.
Members of staff will be made aware of Braunton Academy 's password policy:

- at induction;
- through Braunton Academy online safety policy and password security policy;
- through the acceptable use agreement.

Students will be made aware of Braunton Academy 's password policy:

- in lessons with computing, PSHRE and special events such as Internet Safety Day;
- through the acceptable use agreement.

Audit/Monitoring/Reporting/Review:

The responsible person (Principal) will ensure that full records are kept of:

- User Ids and requests for password changes;
- User logons for 90 days;
- Security incidents related to this policy.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this Braunton Academy.

Responsibilities

The responsibility for the management of the Academy's Filtering policy will be held by the Principal (delegated to Integy). They will manage Braunton Academy filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to Braunton Academy filtering service must:

- be logged in change control logs;
- be reported to a second responsible person (Principal or Lead Teacher);
- be reported to and authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to the Principal any infringements of Braunton Academy 's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by Braunton Academy. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts Braunton Academy to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through Braunton Academy network, filtering will be applied that is consistent with Braunton Academy practice.

- Braunton Academy maintains and supports the managed filtering service provided currently by Integy
- Braunton Academy has provided enhanced/differentiated user-level filtering using the filtering programme
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal
- Mobile devices that access Braunton Academy internet connection (whether Braunton Academy or personal devices) will be subject to the same filtering standards as other devices on Braunton Academy systems
- Any filtering issues should be reported immediately to the filtering provider
- Requests from staff for sites to be removed from the filtered list will be considered by the Principal and Lead Teacher. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Trustee with responsibility for safeguarding

Education/Training/Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the acceptable use agreement;
- induction training;
- staff meetings, briefings, Inset.

Parents will be informed of Braunton Academy 's filtering policy through the acceptable use agreement and through newsletter etc.

Changes to the Filtering System

- Request for changes to the filtering need to be made to the Principal and/or Lead Teacher at least 48 hours before access to the site is required
- There should be strong educational reasons for the request and for the changes to be agreed. If agreed, the changes may allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period;

- Both the Principal and Lead Teacher will be involved to provide checks and balances;
- Any changes made will be recorded in the audit log.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Principal or Lead Teacher will decide whether to make Braunton Academy level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. Braunton Academy will therefore monitor the activities of users on Braunton Academy network and on Braunton Academy equipment as indicated in the academy online safety policy and the acceptable use agreement.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Principal and/or Lead Teacher);
- Safeguarding Trustee;
- External Filtering provider/Local Authority/Police on request.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in academy, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

The Department for Education 'Keeping Children Safe in Education' requires schools to: *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the academy or colleges IT system"* however schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."* In response UKSIC produced guidance on – information on "Appropriate Filtering"

Mobile Technologies Policy (inc. BYOD/BYOT)

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

The absolute key to considering the use of mobile technologies is that the students, staff and wider Braunton Academy community understand that the primary purpose of having their personal device at academy is educational and that this is irrespective of whether the device is Braunton Academy owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only can deepen student learning, but they can also develop digital literacy, fluency and citizenship in students/students that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to Braunton Academy's network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

- Braunton Academy acceptable use agreements for staff, students and parents/carers will give consideration to the use of mobile technologies;
- Braunton Academy allows:

	Braunton Academy devices		*Personal devices*			
	Academy/academy owned and allocated to a single user	Academy/academy owned for use by multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in academy	Yes	Yes	N/A	No	Yes	Yes
Full network access	Yes	Yes			No	No
Internet only					Yes	Yes
No network access						

- Braunton Academy has provided technical solutions for the safe use of mobile technology for Braunton Academy /personal devices (delete/amend as appropriate):
  - all Braunton Academy devices are controlled though the use of Mobile Device Management software;
  - appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access);

[1] Authorised device – purchased by the student/family through a academy-organised scheme. This device may be given full access to the network as if it were owned by the academy

    - Braunton Academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices;
    - for all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted;
    - appropriate exit processes are implemented for devices no longer used at a Braunton Academy location or by an authorised user;
    - all academy/academy devices are subject to routine monitoring;
    - Pro-active monitoring has been implemented to monitor activity.
- When personal devices are permitted:
    - all personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access;
    - personal devices are brought into Braunton Academy entirely at the risk of the owner and the decision to bring the device into Braunton Academy lies with the user as does the liability for any loss or damage resulting from the use of the device in academy;
    - Braunton Academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at academy or on activities organised or undertaken by the academy (Braunton Academy recommends insurance is purchased to cover that device whilst out of the home);
    - Braunton Academy accepts no responsibility for any malfunction of a device due to changes made to the device while on Braunton Academy network or whilst resolving any connectivity issues;
    - Braunton Academy recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the academy. Pass-codes or PINs should be set on personal devices to aid security;
    - Braunton Academy is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
    - devices may not be used in tests or exams;
    - visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements;
    - users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network;
    - users are responsible for charging their own devices and for protecting and looking after their devices while in Braunton Academy;
    - devices must be in silent mode when in classrooms, actively engaged with children or when driving academy buses;
    - Braunton Academy devices are provided to support learning. It is expected that students will bring loaned devices to the academy as required;
    - confiscation and searching (England) - Braunton Academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate;
    - the changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted;
    - the software/apps originally installed by Braunton Academy must remain on Braunton Academy owned device in usable condition and always be easily accessible. From time-to-time Braunton Academy may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps;
    - Braunton Academy will ensure that devices contain the necessary apps for academy work. Apps added by Braunton Academy will remain the property of Braunton Academy and will not be accessible to students on authorised devices once they leave Braunton Academy. Any apps bought by the user on their own account will remain theirs;
    - users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use;
    - users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately;
    - devices may be used in lessons in accordance with teacher direction;

- staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances;
- printing from personal devices will not be possible.

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Braunton Academy recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Braunton Academy, its staff, parents, carers and students.

Scope

This policy is subject to Braunton Academy 's code of conduct and acceptable use agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent Braunton Academy;
- Applies to such online communications posted at any time and from anywhere;
- Encourages the safe and responsible use of social media through training and education;
- Defines the monitoring of public social media activity pertaining to Braunton Academy.

Braunton Academy respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or Braunton Academy 's reputation are within the scope of this policy. Professional communications are those made through official channels, posted on a Braunton Academy account or using Braunton Academy name. All professional communications are within the scope of this policy. Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with, or impacts on, Braunton Academy, it must be made clear that the member of staff is not communicating on behalf of Braunton Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy. Personal communications which do not refer to or impact upon Braunton Academy are outside the scope of this policy.

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
  - Setting up Social Media accounts
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via Braunton Academy accounts
  - Adding an appropriate disclaimer to personal accounts when naming Braunton Academy

Process for creating new accounts

Braunton Academy community is encouraged to consider if a social media account will help them in their work, e.g. a "Friends of the academy" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points: -

- the aim of the account;
- the intended audience;
- how the account will be promoted;
- who will run the account (at least two staff members should be listed);
- will the account be open or private/closed.

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of Braunton Academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by Braunton Academy, including volunteers or parents.

Monitoring

Braunton Academy accounts must be monitored regularly and frequently. Any comments, queries or complaints made through those accounts can only be made whilst in the "open" state. Those responsible for monitoring these accounts need to close the commenting during holiday times. If open, they must be responded to within 48 hours even if the response is only to acknowledge receipt. Regular monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on a Braunton Academy social media account.

Behaviour

- Braunton Academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must always be professional and respectful and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. Braunton Academy social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of Braunton Academy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to Braunton Academy activity.
- If a journalist makes contact about posts made using social media staff must seek advice from the Operations Manager/Principal before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by Braunton Academy and will be reported as soon as possible to a relevant senior member of staff and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with Braunton Academy policies. Braunton Academy does not allow access to private social media sites.
- Braunton Academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, Braunton Academy will deal with the matter internally. Where conduct is considered illegal, Braunton Academy will report the matter to the police and other relevant external agencies and may act according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of Braunton Academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, Braunton Academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken

- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported to the Principal.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging;
- Conversational;
- Informative;
- friendly (on certain platforms, e.g. Facebook).

Use of images

Braunton Academy use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with Braunton Academy's photograph permissions procedure. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via Braunton Academy owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on academy/academy social media accounts. Students/students should be appropriately dressed, not be subject to ridicule and must not be on any academy/academy list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
  - Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with Braunton Academy or impacts on Braunton Academy, it must be made clear that the member of staff is not communicating on behalf of Braunton Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
  - Personal communications which do not refer to or impact upon Braunton Academy are outside the scope of this policy.
  - Where excessive personal use of social media in academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
  - Braunton Academy does not permit access to private social media sites whilst staff are working.
- **Students**
  - **Staff are not permitted to follow or engage with current or prior students below the age of 19 of Braunton Academy on any personal social media network account.**
  - Braunton Academy 's education programme should enable the students/students to be safe and responsible users of social media.
  - Students are encouraged to comment or post appropriately about Braunton Academy. Any offensive or inappropriate comments will be resolved using Braunton Academy's behaviour policy
- **Parents/Carers**
  - **Parents/carers will have access to an academy learning platform where posting or commenting is enabled. Parents/carers will be informed about acceptable use.**
  - Braunton Academy has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on our website.
  - Parents/Carers are encouraged to comment or post appropriately about Braunton Academy. In the event of any offensive or inappropriate comments being made, Braunton Academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to Braunton Academy 's complaints procedures.

Monitoring posts about Braunton Academy

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Braunton Academy.
- Braunton Academy should effectively respond to social media comments made by others according to a defined policy or process.

Managing your personal use of social media:

- “Nothing” on social media is truly private;
- social media can blur the lines between your professional and private life. Don’t use Braunton Academy logo and/or branding on personal accounts;
- check your settings regularly and test your privacy;
- keep an eye on your digital footprint;
- keep your personal information private;
- regularly review your connections – keep them to those you want to be connected to;
- when posting online consider; Scale, Audience and Permanency of what you post;
- if you want to criticise, do it politely;
- take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing Braunton Academy social media accounts

The Do’s

- Check with a senior leader before publishing content that may have controversial implications for Braunton Academy
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.
- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner.
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes using Braunton Academy ’s reporting process.
- Consider turning off tagging people in images where possible.

The Don’ts

- Don’t make comments, post content or link to materials that will bring Braunton Academy into disrepute.
- Don’t publish confidential or commercially sensitive material.
- Don’t breach copyright, data protection or other relevant legislation.
- Consider the appropriateness of content for any audience of Braunton Academy accounts, and don’t link to, embed or add potentially inappropriate content.
- Don’t post derogatory, defamatory, offensive, harassing or discriminatory content.
- Don’t use social media to air internal grievances.

Legislation

Braunton Academy should be aware of the legislative framework under which this online safety policy template and guidance have been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- erase or amend data or programs without authority;
- obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- make unauthorised use of computer time or facilities;
- maliciously corrupt or erase data or programs;
- deny access to authorised users.

Academy/academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- facilitate the secure transfer of information within the European Union;
- prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business;
- give the public confidence about how businesses can use their personal information;
- provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it;
- give data subjects greater control over how data controllers handle their data;
- place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data;
- require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused;
- require the data user or holder to register with the Information Commissioner;

All data subjects have the right to:

- receive clear information about what you will use their data for;
- access their own personal information;
- request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure;
- request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan;

- prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they must follow several set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or another article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, to:

- establish the facts;
- ascertain compliance with regulatory or self-regulatory practices or procedures;
- demonstrate standards, which are or ought to be achieved by persons using the system;
- investigate or detect unauthorised use of the communications system;
- prevent or detect crime or in the interests of national security;
- ensure the effective operation of the system.
- monitoring but not recording is also permissible to:
- ascertain whether the communication is business or personal;
- protect or support help line staff;
- Braunton Academy reserves the right to monitor its systems and communications in line with its rights under this act.

Trademarks Act 1994

This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the academy context, human rights to be aware of include:

- the right to a fair trial;
- the right to respect for private and family life, home and correspondence;
- freedom of thought, conscience and religion;
- freedom of expression;
- freedom of assembly;
- prohibition of discrimination;
- the right to education.

These rights are not absolute. The academy is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Principals (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-academys-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

Southwest Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Academy's

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Principals_and_Academy_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Academys

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in academys

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – Academy Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent forAcademy's– teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AI	Artificial Intelligence
AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Policy History

This Policy is maintained by the Data Protection Officer and will be reviewed on a bi- annual basis, or earlier if needed. For help in interpreting this policy, please contact: DPO Gary Brock

Email: gary@gbrocksolutions.org

Policy Date	Summary of Change	Contact	Implementation Date
Jan 22	Policy updated	DPO Gary Brock	24 March 2022
June 24	• Updated using latest ICO guidance using the SWGFL template • Updated legislation dates as required, • Included new/additional guidance in bold	DPO Gary Brock	2nd June 2024
October 25	• Substantive additions relating to the use of AI and some additions related to cyber security incidents. New flowchart for dealing with incidents of misuse.	DPO Gary Brock	November 2025