Benjamin Britten School

Online Safety Policy

Policy led by: ACo Reviewed: November 2024 Next Review: November 2025

Contents

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This online safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact with on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Sexting.
- Cyberbullying.
- Vulnerability to radicalisation.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social emotional development and learning of the young person.

The breadth of issues classified within online safety is considerable, but can be categorised into 4 areas of risk, according to 'Keeping Children Safe in Education 2025':

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

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

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

The school will deal with such incidents within this policy the 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 school.

Roles and Responsibilities

Key members of staff involved in ensuring that Online Safety is followed alongside the headteachers and governors are:

Imogen Thurbon (Headteacher and Senior Designated Safeguarding Lead / Online Safeguarding Lead)

Aaron Cook (Head of Year and Online Safeguarding Lead)

Ernest Waller (Trust Director of ICT)

Craig Donaldson (IT Technician)

Alex Knights (Primary Designated Safeguarding Lead)

Ashleigh Montgomery (Head of Social Sciences)

Sarah Jarrett (Safeguarding Link Governor)

Network Manager / Technicians

The Network Manager / Technicians are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.

- That the school meets required online safety technical requirements and any Local Authority / other relevant body 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 technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access email is regularly monitored in order that any misuse / attempted misuse can be reported to the school's Online Safeguarding Leads for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.
- Hardware is regularly updated as recommended by Cyber Security hardening techniques.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy.
- They report any suspected misuse or problem for investigation / action / sanction.
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in the curriculum and other activities.
- Students understand and follow the online safety and acceptable use policy.
- 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, camera etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead / Online Safeguarding Lead

The Designated Safeguarding Lead / Online Safeguarding Lead is trained in online safety issues and is 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.
- Cyber-bullying.

Student Acceptable Use Policy

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy. This is signed by the students when they join the school before being given a login.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national + local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website and online student records.
- Their children's personal devices in school and at home.

Community Users

Community users who access school systems as part of the wider provision will be expected to sign the Acceptable Use Policy before being provided with access to school systems.

The use of mobile phones and smart technology

Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college can sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content

It is our expectation that all pupils desist from using smart watches/ devices or mobile phones during the school day but to focus on learning instead. Whilst Smart watches are permitted as long as on do not disturb or flight mode. Any watches that are used as devices will be confiscated and parents will need to collect.

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 is vital strand of safeguarding. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

As a key element of safeguarding staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and are provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / RSHE - Citizenship / other lessons.
- Key online safety messages are reinforced as part of the induction process as well as a planned programme of assemblies and pastoral activities e.g. Safer Internet Day, Wellbeing Wednesday.
- Students are taught in lessons to be critically aware of the materials / content they access online and are guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are helped to understand the need for the student Acceptable Use Agreement (Appendix 1 – Student Acceptable Use Policy) and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies. (Appendix 2 – Staff Acceptable Use Policy).
- In lessons where internet use is pre-planned, the aim is to direct students should to sites checked as suitable for their use.
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Special Educational Needs and Disabilities (SEND)

All academies also have a legal responsibility under the Equality Act 2010 to protect disabled children and those with SEN against direct and indirect discrimination, harassment or victimisation.

At Benjamin Britten Academy we recognise that some pupils with SEND may have difficulties in reporting their experiences of bullying. This may be because they are unable to recognise that they are being bullied, they may not be able to verbalise that they are being bullied or they may experience increased feelings of anxiety which prevent them from 'speaking out'.

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of Online-Safety awareness sessions and internet access.

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 and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Newsletters.
- Parents / Carers sessions
- Campaigns e.g. Safer Internet Day
- Reference to relevant websites / publications
- A dedicated section on the school website.

Education and 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:

- Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable User Agreement.
- The Online Safeguarding 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.
- The Online Safeguarding Lead will provide advice / guidance / training to individuals as required.

Training Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.
- Online training modules through National College

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our students' lives, not just in school but outside as well, and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present. We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and students will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons. We will remind students about the responsibilities to which they have agreed through the Acceptable Use Policy. Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies

Education / Training / Awareness

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

- The Acceptable Use Agreement
- Induction training.
- Staff meetings, briefings, PD Days.

Technical – Infrastructure / Equipment, Filtering and Monitoring

Managing and Safeguarding IT Systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible. Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

All administrator or master passwords for school IT systems are kept secure and available printed in the safe in the school office. The wireless network is protected by a secure log on which prevents unauthorised access. New users can only be given access by named individuals e.g. a member of technical support. We do not allow anyone except technical staff to download and install software onto the network.

Filtering Internet Access

Web filtering of internet content is provided by Smoothwall. This ensures that all reasonable precautions are taken to prevent access to illegal content. However, it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in students in monitoring their own internet activity. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. There is differentiated filtering for students, staff and administrators. Teachers are encouraged to check out websites they wish to use prior to lessons for the suitability of content.

Audit / Reporting

Smoothwall logs show internet activity that has taken place within the last week. This will be made available to:

- Online Safeguarding Leads.
- Safeguarding Governor.
- External filtering provider / Police on request.
- The filtering policy will be reviewed in the response to the evidence by the Smoothwall log or suitability of the current provision.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Trust Director of ICT. They will manage the school 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 the school filtering service must:

- Be logged.
- Be reported to a second responsible person.

All users have a responsibility to report immediately any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However, deliberate access of inappropriate or illegal material will be treated as a serious breach of the Acceptable Use Policy and appropriate sanctions taken. 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.

Access to School Systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted for internet access.

All users are provided with a log in appropriate to their role in school. Students are taught about safe practice in the use of their log in and passwords. Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords. Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information. Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

Passwords – Follows Microsoft Policy

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).

- Students get to choose their own password.
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All students have a unique, individually-named user account and password for access to IT equipment and information systems available within school. All staff and students have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains a log of all accesses by users and of their activities while using the system in order to track any online safety incidents.
- Internet activity is automatically logged by Smoothwall.

Using the Internet

We provide the internet to:

- Support curriculum development in all subjects.
- Support the professional work of staff as an essential professional tool.
- Enhance the school’s management information and business administration systems.
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others.
- Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.
- All users of the school ICT or electronic equipment will abide by the relevant Acceptable Use Policy at all times, whether working in a supervised activity or working independently.
- Students and staff are informed about the actions to take if inappropriate material is discovered and this is supported by guidance placed on every lesson PowerPoint in the Computing curriculum.

Websites

- 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.
- Staff will preview any recommended sites before use.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff.
- All users must observe copyright of materials published on the Internet.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment.

- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- Staff should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Using Email

Email is an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, students and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

Use of the school e-mail system is monitored and checked. It is the personal responsibility of the email account holder to keep their password secure. As part of the curriculum students are taught about safe and appropriate use of email. Students are informed that misuse of email will result in a loss of privileges. Under no circumstances will staff contact students, parents or conduct any school business using a personal email address.

Use of Digital and Video Images

The Data Protection Act 1998 affects the official use of photography by educational settings, as an image of a child is considered to be personal data.

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 cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes without permission.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.
- 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.
- The school record of parental permissions granted/not granted for the use of photographs of students must be adhered to when taking images of our students. A list is available from the main office.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). Unless stated. For example, shows run by the Performing Arts department. 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.
  When student images are to be used in the media (e.g. newspapers or TV) or for other extraordinary use specific consent will be obtained.
  Student are not permitted to wear smartwatches during examinations.

Using other Technology

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an online safety point of view. We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by students. Staff or students using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Online Teaching and Learning

Online learning and safeguarding protocols for virtual/'live' teaching. Guidance for staff and raising awareness for parents/carers. These protocols focus on:

- Pre-recorded screen, video and/or audio lessons.
- Using comments in Google Classroom.
- Running live lessons via Google Classroom.

Pre-recorded Screen Recordings, Video and/or Audio Lessons Protocols:

Voice recording – this is where you record yourself talking through an activity, model or giving feedback. Ensure you speak using formal English in the way you would in a normal classroom. Only use a student's name if you are praising individual work.

Screen recording – this is where you share with students a recording of your computer desktop. Ensure that the video does not record any personal background/information. You can do this by either changing the settings on your recording to record a 'window' or a 'tab' only OR ensuring you have a neutral background, and there is no personal information available (i.e. nothing saved to the desktop).

Video recording – this is when you record yourselves talking through an activity, explaining a model or giving feedback. It is your choice whether you choose to turn the video on or not in these videos. If you choose to turn video on, please ensure that:

- The background is neutral and professional. At all times the setting should be in a location suitable for delivery of a video lesson e.g. a living space or a study area. Videos should not be recorded in a bedroom and should not include other adults or children in the background.
- Teacher dress code is the same as it is in school – smart and professional.

Using Comments in Google Classroom

- Use academic English in your comments to students.
- Students must use academic English at all times and only comment on the work.
- Any inappropriate comments will be recorded in a screenshot and sent to the relevant Year Team, who will communicate with parents.
- Ensure any behaviour concerns are recorded in Bromcom, where appropriate they are reported to the Head of Department / Year Team.
- If students are not following the expectations you have of them, they can be muted in Google Classroom, so they can no longer make comments.
- Ensure any welfare/safeguarding concerns that arise during the communication are recorded and reported straight away on Bromcom.

Running Live Lessons via Google Classroom

Protocol for Teachers:

- Staff must only use platforms provided by Benjamin Britten Music Academy to communicate with students once they have taken part in live lesson training i.e. no communication with students should be done using your mobile phone, WhatsApp, any other social media platform etc.
- Security settings must be enabled.
- Teacher dress code is the same as it is in school – smart and professional.
- If teacher camera is on, the background must be neutral and professional. At all times the setting should be in a location suitable for delivery of a video lesson. Any computers used should be in appropriate areas, for example, not in bedrooms and should not include other adults or children in the background.
- Staff can record live lessons provided that children cannot be seen or heard.
- Staff are advised to consider screen time for both themselves and the students.
- Language must be professional and appropriate.
- Staff need to ensure they are the organiser of the Google Classroom live lesson and close the video once the lesson is over so students cannot contact each other without supervision.
- Staff should not enter a Google Meet that has been set up by a student.

Protocol for Students

- Students must only join using their school account through Google Classroom.
- Students must only join the class once the teacher has announced it live on the google classroom stream.
- Students must mute their microphones unless asked to unmute by the teacher.
- If students have a question, they can write ‘question’ or type the question into the comment box or press the raised hand button.

- All comments made by students must be focused on the work and be relevant to the lesson being taught.
- Teachers can see the comments so students must write in an appropriate way at all times i.e. use academic English at all times.
- At no point, should students take any form of recording or photo of the session. If it is found that this has happened, it will immediately be referred to the Year Team and students will face serious sanctions in line with our behaviour policy.
- In live lessons students and any parent in view must be in appropriate clothes and have a neutral and appropriate background (e.g. they must not be in a bedroom or have any siblings or other family members in the background).
- At the end of the lesson you must, end the recording, leave the lesson and close the window.

Behaviour Systems to Support these Protocols

Any students who don't follow our protocols will be subject to one or more of the following sanctions:

- The student(s) in question will be muted in the classroom by the teacher.
- The student(s) in question will be removed from the classroom by the teacher. The Head of Department and relevant Head of Year will be notified via the behavioural referral system and we will also contact home.
- If necessary, the lesson will be stopped and closed.
- Sanctions will follow the school's behaviour policy.

All lessons are recorded and saved by the school in line with our data protection policy which is available to parents, carers and children on the school website.

Communication

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

		Staff and other adults					Students and young people			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not permitted
Mobile phones may be brought to school		**X**						**X**		
Mobile phones used in lessons			**X**					**X**		
Use of mobile phones in social time		**X**								**X**

Taking photographs on mobile devices				X						X
Use of other mobile devices e.g. tables, gaming devices		X							X	
Use of school email for personal emails					X					X
Use of school web based email e.g. outlook		X					X			
Social use of online “chat” platforms					X					X
Use of social network sites			X							X
Use of educational blogs		X					X			

Additional Information on the use of Communications Technologies

When using communication technologies:

- The official school email service may be regarded as safe and secure and is monitored.
- Users must immediately report 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

Students are not allowed on social networking sites at school. Social media sites are blocked by the school’s filtering systems. However, students and staff may have social media accounts which they use out of school. School social media accounts are permitted providing they have permission from the Headteachers. With this in mind the following guidance is to be followed:

School staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Members of staff must not use social media on school devices except for specific educational purposes where permission has been granted.
- Social networking is only allowed in school on the personal devices of members of staff in accordance with the online safety and staff conduct policies.
- Members of staff must not “friend / follow” or otherwise contact current students or parents / carers through social media.
- Current students attempt to “friend / follow” or otherwise contact members of staff through social media, they should be reported to the Senior Designated Safeguarding Lead. Staff must not allow current students to “follow” them, for instance on Instagram.
- Members of staff must not post content online which is damaging to the school or any of its staff or students.

Student and parents / carers:

- Students may not access social media whilst in school.
- Breaches of this policy by students will be taken seriously and dealt with according to the behaviour policy.
- Current students and parents / carers must not attempt to “friend”/”follow” or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they must be reported to the Online Safeguarding Leads and Senior Designated Safeguarding Lead.
- If members of staff attempt to “friend” or otherwise contact current students or parents / carers through social media, they should be reported to the Online Safeguarding Leads and Designated Safeguarding Lead.
- If inappropriate content is accessed online on school premises, it must be reported.
- Attempts to circumvent the network’s firewalls will result in a ban from using school computing equipment, other than with close supervision.
- Students in the KS3 ICT curriculum will be taught about online safety within the Computing, RSHE curriculum and within pastoral programs.
- Students must not post content online which is damaging to the school or any of its staff or students.

Staff are not authorised to create any blog / networking page, etc. representing the school without permission.

Dealing with Online Safety Incidents

All online safety concerns are recorded as a safeguarding incident on Bromcom using the internet safety concern alongside any other relevant category. This log is reviewed once a term in strategic Designated Safeguarding Lead meetings and the facts and figures are analysed. This information is shared with governors in the form of a report. Risk assessments are carried out as appropriate in response. Staff are encouraged to report online concerns as a safeguarding incident via Bromcom. Any incidents where students do not follow the Acceptable Use Policy will be dealt with following the school’s normal behaviour or disciplinary procedures. Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. The school recognises that staff as well as students may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safeguarding Leads and Designated Safeguarding Leads. Technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing our safeguarding policy (including the Acceptable Use Policy) and procedures. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that student data has been lost. The school reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with Issues Arising from the Use of Technology

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- Accessing inappropriate or illegal content deliberately.
- Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned.
- staff using digital communications to communicate with students in an inappropriate manner (for instance, communication via social networking sites).

The following activities are likely to result in disciplinary action:

- Any online activity by a member of the school community which is likely to adversely impact on the reputation of the school.
- Inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons.
- Sharing files which are not legitimately obtained e.g. music files from a file sharing site.
- Circulation of commercial, advertising or 'chain' emails or messages.
- Revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission.
- Using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content).
- Transferring sensitive data insecurely or infringing the conditions of the Data protection Act, revised 1988.

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve.

- Accessing social networking sites, instant messaging accounts or using a mobile phone for personal use during lesson time.
- Sharing a username and password with others or allowing another person to log in using your account
- Accessing school ICT systems with someone else's username and password.
- Deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else.

Sharing of Semi-Nudes

In advice for schools and colleges (UKCIS, 2020), sexting is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

Incidents involving sharing nudes and semi-nudes should have an immediate focus on safeguarding children. The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to a Designated Safeguarding Lead and the police as a matter of urgency.

If a member of staff has a report of or suspects the sending or sharing of a semi-nude, it is important to remember that intimate images are typically considered to be illegal images which is why incidents need very careful management for all those involved. Any 'Youth Produced Sexual Imagery' (YPSI) incident in school must be treated as a safeguarding issue. It is against the law to create, send and share indecent images of a person under the age of 18.

What to do if an incident comes to your attention

If an incident comes to your attention, you must report it to the Designated Safeguarding Lead (DSL) immediately and record the incident on Bromcom.

- Never view, copy, print, share, store of save the imagery yourself, or ask a child to share or download. This is illegal.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

If a device is involved it is essential to secure the device and switch it off. The matter must then be reported to the school's DSL and Online Safeguarding Leads. Staff should not view any YPSI images / video (YPSI = Youth Produced Sexual Imagery).

All incidents of semi-nude images must be recorded with an explanation of actions taken. In applying judgement to each semi-nude image incident, the following must be considered:

- Any significant age difference between the sender/receiver involved.
- If there is any external coercion involved or encouragement beyond the sender/receiver.
- If the child is recognised as more vulnerable than is usual (i.e. at risk).
- If the image is of a severe or extreme nature.
- If the situation is not isolated and the image has been more widely distributed.
- If other knowledge of either the sender/recipient may add cause for concern (i.e. difficult home circumstances).

Schools may respond to a YPSI incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

If the DSL is confident that they have enough information to assess the risks to any child or young person involved and the risks can be managed within the education setting's pastoral support and disciplinary policy. If a referral is made to the police, children involved in sexting incidents will be dealt with (by the police) as victims as opposed to perpetrators (unless there are mitigating circumstances). In the majority of cases, parents / carers should be informed of their child being involved in a YPSI incident.

NOTE: Youth Produced Sexual Imagery (YPSI) – For the purposes of this advice 'youth' refers to anyone under the age of 18.

Unsuitable / Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school 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,	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					**X**

remarks, proposals or comments that contain or relate to:	Contrary to the Sexual Offences Act 2003.					
	Possession of an extreme pornographic image (grossly offensive 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	X
	threatening behaviour, including promotion of physical violence or mental harm.				X	X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.				X	
Sites which may promote radicalisation.						X
Using school systems to run a private business.					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy.					X	
Infringing copyright.					X	X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).					X	
Creating or propagating computer viruses or other harmful files.					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet).					X	
Online gaming (educational).			X			
Online gaming (non-educational).			X			
Online gambling.					X	
Online shopping / commerce.				X		
File sharing.				X		
Use of social media.			X*			
Use of messaging apps.			X			

* in accordance with the school's safety and staff conduct policies.

Responding to Incidents of Illegal Misuse

If any apparent or actual misuse appears to involve illegal activity the flow chart below is consulted and followed. Incidents will never be tolerated and the Police will be involved. Illegal activity would include:

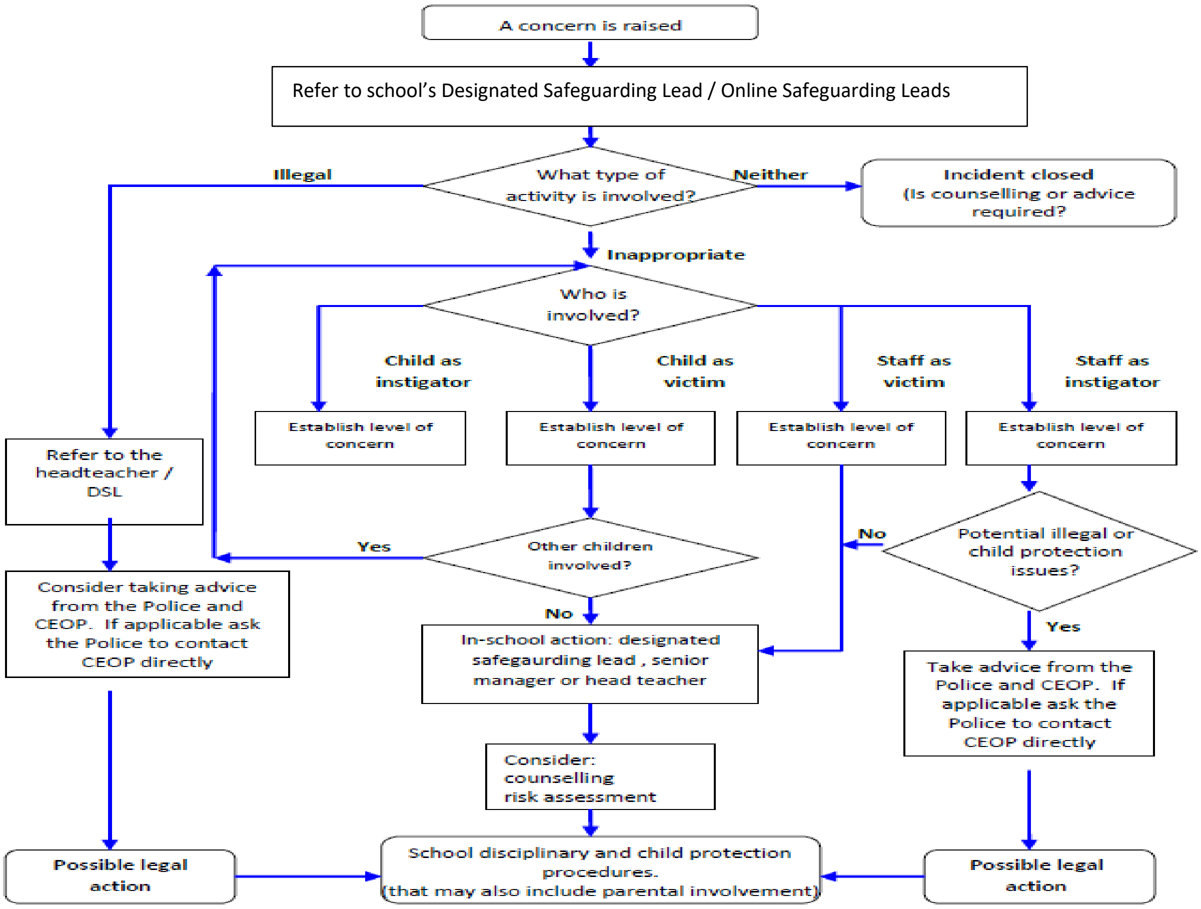
- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

If members of staff suspect that illegal misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such an event it is recommended that more than one member of staff is involved in the investigation.

In cases of suspected illegal misuse.

Note: NEVER investigate yourself or view images. Refer the matter immediately. DO NOT let others handle evidence.

Response to an Incident of Concern (Illegal Misuse)


A concern is raised
Refer to school's Designated Safeguarding Lead / Online Safeguarding Leads
Illegal
What type of activity is involved?
Neither
Incident closed (Is counselling or advice required?
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern
Establish level of concern
Establish level of concern
Establish level of concern
Refer to the headteacher / DSL
Yes
Other children involved?
No
Potential illegal or child protection issues?
Consider taking advice from the Police and CEOP. If applicable ask the Police to contact CEOP directly
No
In-school action: designated safegaurding lead , senior manager or head teacher
Yes
Take advice from the Police and CEOP. If applicable ask the Police to contact CEOP directly
Consider: counselling risk assessment
Possible legal action
School disciplinary and child protection procedures. (that may also include parental involvement)
Possible legal action

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 or national / local organisation (as relevant).
- Police involvement and/or action.

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

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

Monitoring and Evaluation

The Designated Safeguarding member of SLT, Online Safeguarding Leads and governor will be responsible for ensuring that this policy is monitored and evaluated regularly. The safeguarding leads will regularly discuss matters relating to the monitoring of the online safety policy including the impact of initiatives, the filtering policy, incidents and the 360-degree safe self-review tool. The policy and procedures are aligned with the Child Protection, Behaviour and Anti-Bullying Policies. This policy will be reviewed annually and may be subject to change without notice. It will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix

Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview