Bradford Christian School

Online Safety Policy

Written May 2018 – Review date October 2021

1.0 **Statement**

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

1.2 The Education and Inspections Act 2006 empowers Headteachers to such an 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 published Behaviour & Discipline Policy.

1.3 The school 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 school. The vulnerability of children is a central concern in this policy and our commitment is to safeguard the children in our care.

1.4 We aim to protect and educate students and staff on their safe and wise use of technology. To have appropriate mechanisms to intervene and support students and deal effectively with any incident that occurs in school. To combat the following three areas of e-safety risk

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subject to a harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of or causes harm to self or others.

1.5 The aim of this policy is to keep all users of technology in school safe. As a school we recognise that sometimes we all make mistakes, however we ask that when and if that occurs that you talk to a senior member of staff as soon as possible should it occur.

2.0 **Roles and Responsibilities**

2.1 **Governors** 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 Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, Simon MacKenzie. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Officer Mr Shaun McGrail
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting
- discussing the online safety policy with governors for input into the published policy

2.2 **The Headteacher** has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer (Shaun McGrail).

- The Headteacher and the School Business Manager will be responsible for the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or member of the school community. (see flow chart on dealing with online safety incidents (Page 9) and Responding to incidents of misuse (Page 9)
- Incidents of concern can be reported either through the Whisper Button which is available to all staff, students and parents or using the pink safeguarding reporting form.
- The Headteacher and Senior Leadership Team (SLT) are responsible for ensuring that the Online Safety Officer receives suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

2.3 **The Online Safety Officer:**

- leads the discussions re online safety across the school community e.g. at student forums, with the online safety governor, at teacher inset days and in communication with parents through the online parent zone.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy.
- 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
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports termly to the Senior Leadership Team
- ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ensures that users may only access the networks and devices through a properly enforced password protection policy, (see Technical security policy for detail)
- ensures the filtering policy is applied and updated on a regular basis (see Technical security policy for detail)
- keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- ensures that the use of the network / internet / Google Classroom / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / SLT for investigation / action / sanction
- ensures that monitoring software / systems are implemented and updated.

2.4 **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
- annually they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher/ Online Safety Officer / Designated Safeguarding Lead 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 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 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 0searches

2.5 **Designated 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

2.6 **Students:**

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement to be completed annually.
- 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 know and understand school policies on the use of mobile devices and digital cameras. They will also know and understand policies on the taking / use of images and on cyber-bullying.
- will 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

2.7 **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, Google classroom and information about national / local online safety campaigns / literature and the school parent zone on the web page. 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 / Google classroom and on-line student / pupil records
- their children's personal devices in the school

3.0 **Education and Training**

3.1 **Students**

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

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

- A planned online safety curriculum will be provided as part of Computing / PHSE / other lessons and will be regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will 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 will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will 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 will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will 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 will 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 will 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 the On line safety officer 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.

3.2 **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 on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, Parent Zone on the school web site
- 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

3.3 **Staff / Volunteers**

Staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal 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 annually during staff reviews**.**
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Officer will receive regular updates through training material 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 meetings.

3.4 **Governors**

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any group involved in online safety / health and safety /safeguarding through participation in school training / information sessions for staff

4.0 **Technical – infrastructure / equipment, filtering and monitoring**

4.1 The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that the technical security policy and procedures are implemented. The school will ensure that the relevant people named in the above sections are effective in carrying out their online safety responsibilities.

4.2 No filtering system can guarantee 100% protection against access to unsuitable sites. Therefore, School technical staff will regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

4.3 Whisper is in place for users to report any actual / potential technical incident / security breach to Mr Shaun McGrail.

4.4 All staff devices and phones in school should be password protected and all security incidents are reported via the existing safeguarding procedures or via whisper.

4.5 An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This is restricted access that is monitored and by Mr McGrail.

4.6 Staff may use school devices out of school provided the device is protected with up to date viral protection and is password protected.

4.7 Staff are able to download the executable files in the list below from a secure webpage not from an e-mail. Any other executable files should first be checked with the online safety officer before they are downloaded.

- Adobe
- Flashplayer

4.8 Staff are able to use removable media (e.g. memory sticks / CDs / DVDs) on school devices. However they should be encrypted and stored securely in school and should not be removed from school. Users should move towards storage of information on the cloud rather than removable media.

4.9 Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

5.0 **Use of digital and video images**

5.1 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.

5.2 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 will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will 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 school 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 school 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 or 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 school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless specific permission has been given by SLT to use their own device for a specific event and the appropriate steps have been taken to download the images to the school intranet and delete them from their personal device upon return to school.
- Care will be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.

6.0 **Communications**

6.1 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.

Communication Technologies	Staff & other adults				Students			
	Allowed	Allowed at certain times	Allowed when directly related to teaching	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	✓						✓	
Smart Watches (internet/phone enabled)	✓							✓
Use of mobile phones in lessons			✓				✓	
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓
Use of social media				✓				✓
Use of blogs			✓					✓

6.2 When using communication technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to Mr Shaun McGrail – in accordance with the school 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) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses will be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use.
- Students will be taught about online safety issues, such as the risks attached to the sharing of personal details and strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

7.0 **Social Media - Protecting Professional Identity**

7.1 All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Please see the staff code of conduct for further information.

7.2 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

7.3 School staff will ensure that:

- No reference will be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not be attributed to the school
- When using social media staff will be aware that personal views expressed on a personal social media account are public and will ensure that comments made are appropriate and do not bring the school into disrepute by association.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

7.4 The school's use of social media for professional purposes will be checked by the senior risk officer to ensure compliance with school policies.

8.0 **Unsuitable / inappropriate activities**

8.1 Any internet activity that is illegal e.g. accessing child abuse images or distributing racist material is banned from school and all other technical systems. We do not tolerate cyber-bullying or any other inappropriate activity and the appropriate action will be taken in all instances in line with the School Discipline and anti-bullying policy or referral to the Police as appropriate. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

8.2 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 / or outside the school / when using school equipment or systems. The school policy restricts usage as follows: (see table below)

User Actions

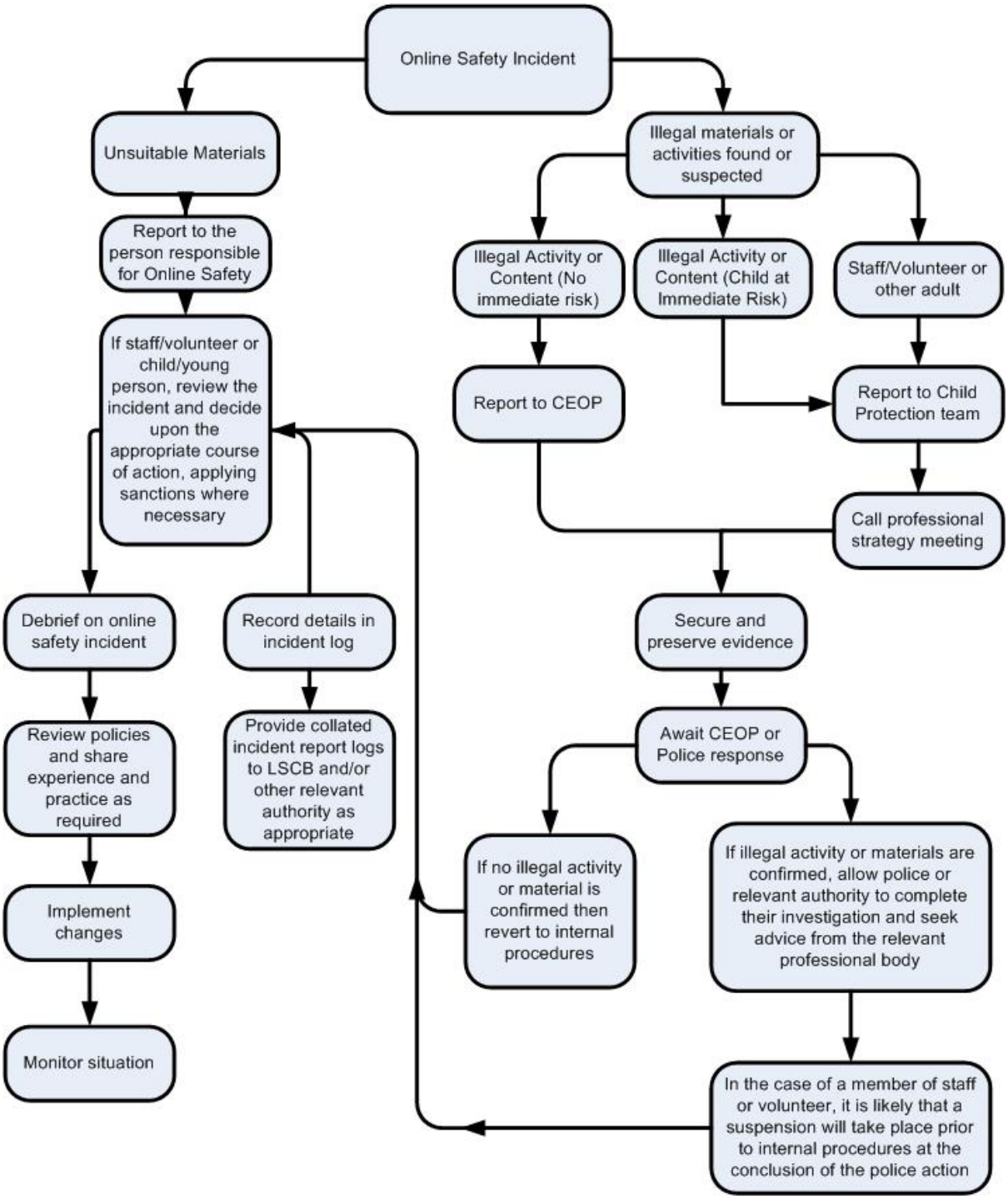
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Users shall not visit Internet sites, make, posts, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production 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 other wise of obscene character) contrary to the Criminal Justice & 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 the school or brings the school into disrepute				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					X
Infringing copyright					X
Revealing or publicising confidential or proprietary information (eg 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
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		

9.0 **Responding to incidents of misuse**

9.1 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).

9.2 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.



9.3 **Other Incidents**

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

9.4 **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 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 2019
    - criminally racist material
    - promotion of terrorism or extremism
    - 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

10.0 **School Actions & Sanctions**

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

Student Incidents

	Actions / Sanctions								
	Refer to Head of Department	Refer to Designated Safeguarding lead	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / 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		X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	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	X	X
Allowing others to access school network by sharing username and passwords	X		X		X	X		X	X
Attempting to access or accessing the school network, using another student's account	X		X		X	X		X	X
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X	X		X	X
Corrupting or destroying the data of other users	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	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school'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	X		X	X

Staff Incidents

	Actions / Sanctions							
	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action	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	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X	X	X
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school 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
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	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
Carrying out digital communications with students via non-school accounts or systems, including email, social networking, instant messaging, text messaging, etc.	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 the school into disrepute or breach the integrity of the ethos of the school	X	X				X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X	X

11.0 **Review of this Policy**

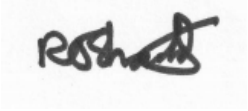
11.1 In writing this policy Bradford Christian school acknowledges:

- the materials supplied and used from SWGfL Online Safety School Template Policies
- The Education and Inspections Act 2006
- General Data Protection Regulations
- The 2011 Education Act

11.2 This policy should be read in conjunction with the following school policies:

- Technical security policy
- Data Protection Policy
- Behaviour and Discipline Policy (students)
- Discipline Policy (staff)
- Safeguarding and Child protection policy
- Preventing extremism and radicalisation policy
- Anti-Bullying Policy
- Staff code of conduct

11.3 This policy is reviewed annually this latest review being completed in November 2020.

Formally agreed through Governors compliance:	**14th January 2021**
Signed Richard Shackleton – Chair of Governors	
Signed Jane Prothero – Head Teacher	
Review Date:	**October 2021**

Bradford Christian School Student Acceptable Use Agreement – for older students (Upper School)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. 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 internet access at all times.

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 school 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.

Student Acceptable Use Agreement

I understand that I must use ICT school 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 the school will monitor my use of the systems, devices and digital communications.
- I will treat my username and password like my toothbrush I will not share it, I will keep it safe and secure. 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 strangers I have only met on line.
- 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 the school 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 the school 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 not steal, disable or cause damage to school equipment or the equipment belonging to others.
- I will not use personal email addresses on the school ICT systems.

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 the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- 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 school device, nor will I try to alter computer settings.
- I will only use social media sites with permission.

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 school:

- I understand that the school 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 school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- I understand that sometimes we all make mistakes, however If I do make a mistake I will talk to a senior member of staff as soon as possible about it.

Please complete the section on this page to show that you have read, understood & agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems & devices.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: .....

Year Group: .....

Signed: .....

Date: .....

Parent / Carer Countersignature .....

Bradford Christian School Student Acceptable Use Policy Agreement– for younger pupils (Primary and Middle School)

I understand that I must use the school devices carefully and treat them with respect.
I understand that when I use the internet at school I must be careful to follow the school rules that are in this agreement.
I understand that sometimes we all make mistakes, however If I do make a mistake I will talk to a senior member of staff as soon as possible about it.

This is how I will stay safe when I use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me or makes me worried or scared on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I understand that the school will be watching what I do online.
- I will be aware of 'stranger danger' when I am talking to people or characters online.
- I will report any damage to the laptops or things that have go wrong, however this may have happened.

I will act as I expect others to act toward me:

- I will respect others' work and the things that belong to them.
- I will not change their work or delete anything that belongs to them.
- I will not take pictures or send them to anyone else without their permission.

I understand that if I break this agreement I will be disciplined.

Signed (child):……..Year Group……..

Signed (parent):……..Date:……

Appendix C

Bradford Christian school Parent / Carer Acceptable Use Agreement

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

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 school 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 with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning & will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

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

I understand that the school 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 school.

I understand that the school 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 the school 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 the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

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

Signed: .....

Date: .....

Bradford Christian School Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with The general data protection regulations and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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). **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**.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

As the parent / carer of the above student , I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Use of Cloud Systems Permission Form

The school uses Google Apps for Education for students and staff. This permission form describes the tools and student responsibilities for using these services. The following services are available to each student and hosted by Google as part of the school's online presence in Google Apps for Education:
Mail - an individual email account for school use managed by the school
Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments
Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
Sites - an individual and collaborative website creation tool
Using these tools, students collaboratively create, edit and share files and websites for school related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others. The school believes that use of the tools significantly adds to your child's educational experience.
As part of the Google terms and conditions we are required to seek your permission for your child to have a Google account.

As the parent / carer of the above student, I agree to my child using the school using Google Apps for Education.	Yes / No

Signed: .....

Date: .....

Appendix E

Bradford Christian School Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

The school 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 school 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 the school will monitor my use of the school 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 school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school 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 the school.
- 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 school ICT 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 &/or publish images of others I will do so with their permission and in accordance with the school'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 the school 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 school in accordance with the school's policies.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, 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 school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted 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 school 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.
- I will not take photos of students on my own device and will only take photos on school devices for valid educational reasons.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.
- I understand that sometimes we all make mistakes, however If I do make a mistake I will talk to a senior member of staff as soon as possible about it.

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

Staff / Volunteer Name: .....

Signed: ..... Date: .....

Appendix F

Bradford Christian School - Responding to incidents of misuse Record

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

Group: .....
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

Bradford Christian School Reporting Online Safety Incidents Log						**Appendix F**
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Bradford Christian School Staff Online Safety Training Needs Log				**Appendix G**
Name of Staff Member	Identified Training Need	To be met by	Date	Review Date