CATHEDRAL SCHOOLS TRUST | BRISTOL CATHEDRAL CHOIR SCHOOL

Gathered together, that all may thrive

Policy Name:	BCCS Online Safety Policy
Review Cycle:	Annually
Author:	David Bugler
Lead Governor:	Beth Williamson
Approved by / Date:	Stephen Fuller, Designated Safeguarding Lead - 16.11.22 Beth Williamson - 21.11.2022

Date	**Summary of Changes**
Nov 2022	- Roles and Responsibilities updated - 'Teaching of E Safety' section added - Managing mobile phones and other personal devices updated

BCCS Online Safety Policy

MISSION STATEMENT

Bristol Cathedral Choir School is a Church of England Academy with an ethos reflecting the Christian faith and with music and mathematics as its specialisms.

It aspires to be a learning community where all achieve their full potential in a supportive and tolerant environment, so that they can contribute fully to the society in which they live.

Background

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. The risks associated with online activity are complex and varied, from breaches in personal data and identity theft to cyber bullying, blackmail and radicalisation.

Roles and Responsibilities Surrounding E Safety

Bristol Cathedral Choir School's Designated Safeguarding Lead (DSL) acts as the designated e-safety lead. His or her responsibilities include:

- Supporting the Headteacher in ensuring that staff understand the e-Safety policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, IT manager and other staff, as necessary, to address any e-safety issues or incidents.
- Ensuring that e-safety incidents are logged onto CPOMS and dealt with appropriately.
- Ensuring that incidents of cyberbullying are logged and dealt with in line with the School's Behaviour Policy and the Trust's Anti bullying policy.
- Organising, updating and delivering staff training on e-Safety.
- Completing e-Safety audits annually (see appendix one)
- Liaising with other agencies and services as necessary (see appendix two for a list of helpful contacts).
- Providing regular reports on e-Safety to the Headteacher and Governors.

The Lead Governor for e-Safety is **Beth Williamson.**

The DSL must be made aware of any disclosures, incidents or Child Protection concerns. The Senior Leadership Group and Governing Body must be involved and should review the e-Safety policy annually and monitor its impact. They will also need to ensure that

they take responsibility for revising the e-Safety policy and practice where necessary (such as after an incident or change in national legislation).

The Governing body has a legal responsibility to safeguard children and staff and this includes online activity.

Teaching and learning

1. Why Internet use is important

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote Student achievement, to support the professional work of staff and to enhance the school's management functions.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between Students worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for Students and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of administration data with DfE;
- Access to learning wherever and whenever convenient.

Internet use enhances learning:

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and Students complies with copyright law.

- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of Students.
- Staff should guide Students to online activities that will support the learning outcomes planned for the Students' age and ability.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1. Teaching of E-Safety

Students will be taught about e-Safety as part of the curriculum through the school's PSHE Programme, assemblies and guest speaker events. This will include:

- How to use technology safely, respectfully and responsibly.
- The acceptable and unacceptable behaviour surrounding online activity and, in particular, social media platforms.
- How to report a range of concerns, both at school and to other organisations.
- How changes in technology affect safety, including new ways to protect online privacy and identity.
- The implications of digital footprints on everyday life and future careers.
- The dangers of the uncritical acceptance of 'fake news' and other information that is intended to radicalise towards a particular extreme ideology.

The school will also raise awareness of the internet safety to parents through regular communications home, information via the school's website and e-Safety webinars.

All staff will receive training through the induction process or annual refresher training with updates provided as required.

Managing Internet Access

2. Information system security

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT network manager (Tom Bliss) will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

3. Email

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a designated member of staff if they receive an offensive email.

- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with Students and parents/carers, as approved by the Senior Leadership Group.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

Published content and the school website:

- The contact details on the website should be the school address, email and telephone number. Staff or Students' personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- Paul Herbert (Edge Media) will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

4. Publishing students' images and work

Please also see sec 2.3 Staff and Volunteer Acceptable Use Policy Agreement, *Communications Policy*

- Images or videos that include Students will be selected carefully and will not provide material that could be reused.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of Students are electronically published.
- Students' work can only be published with their permission or that of their parents.
- Written consent will be kept by the school where Students' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which asks parents' permission of use.

5. Social networking and personal publishing

- The school will attempt to control access to social media and social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will seek consent from the Senior Leadership Team before using Social Media tools in the classroom if unsure.
- Staff official blogs or wikis should be password protected and run with knowledge and with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for Student use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Handbook.

6. Managing Filtering

- The school's broadband access will include filtering appropriate to the age and maturity of Students.
- The school will ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all Students) will be aware of this procedure.
- If staff or Students discover unsuitable sites, the URL will be reported to the School eSafety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Group.
- The School Senior Leadership Group will ensure that regular checks are made to ensure that the filtering methods selected are effective.

- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Bristol Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the Students, with advice from network managers.

7. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Communications Policy.

8. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

9. Authorising Internet access

- The school will maintain a current record of all staff and Students who are granted access to the school's electronic communications.
- All staff will read and sign the School Acceptable Use Policy (see *Communications Policy*) before using any school ICT resources.
- Students will apply for Internet access individually by agreeing to comply with the Acceptable Use Policy.
- Parents will be asked to read the School Acceptable Use Policy for Student access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that Students will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the Student(s).

10. Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Bristol Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

11. Responding to incidents of concern

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Bristol.

12. Handling e-Safety complaints

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Students and parents will be informed of the complaints procedure.
- Parents and Students will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

13.The internet across the community

- The school will liaise with local organisations to establish a common approach to e–Safety.
- The school will be sensitive to Internet-related issues experienced by Students out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Managing Cyberbullying:

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Anti-bullying Policy and Behaviour Management Policy.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for Students and staff may also be used in accordance to the school's anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parents/carers of Students will be informed.
    - The Police will be contacted if a criminal offence is suspected.

14.Managing BCCS Platforms- Classcharts, subject specific platforms, classcharts

- The DSL and staff will regularly monitor the usage of the Classcharts by Students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using platforms.

- Only members of the current Student, parent/carers and staff community will have access to Classcharts.
- All users will be mindful of copyright issues and will only upload appropriate content onto Classcharts and other platforms.
- When staff, Students etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on any platforms may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the platform for the user may be suspended.
  d) The user will need to discuss the issues with a member of SLG before reinstatement.
  e) A Student's parent/carer may be informed.
- A visitor may be invited onto a platform by a member of the SLG. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the Student to fulfil a specific aim and may have a limited time frame.

15.Managing mobile phones and other personal devices

- The use of mobile phones and other personal devices by students in Years 7 - 11 is prohibited in school (in class and around the site) from 8:40am – 3:20pm and should be used by teacher invite only to support learning. If a student does not adhere to this, school staff may confiscate a phone or device. If confiscated the phone will be kept in a secure place or handed to HOH or SLT. The student may then go and collect at 3:20pm from the front reception or teacher. If a student has their phone confiscated frequently, the phone will be kept until a parent or carer comes in to sign for the phone or device.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school Behaviour and Management Policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership or House Teams with the consent of the Student or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and at Failand.

16. Students Use of Personal Devices

- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a Student needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

17. Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with Students or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Group in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then the advice is to seek the approval of the Subject Leader, HOH or SLT.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of Students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

18.Communicating the Policy to Students

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
- Student instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and ICT programmes covering both safe school and home use.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access as well as be accessed during sign on
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where Students are considered to be vulnerable.

19.Communicating the policy with staff

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and Students, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by DJB and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the Students.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

20.Parental Support

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet AUP agreement as part of the use on Parental Portal
- Parents will be encouraged to read the school Acceptable Use Policy for Students and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "e–Safety Contacts and References section".

Schools e-Safety Audit

This suggested self-audit will be completed by a BCCS Staff member in consultation with all stakeholders.

Has the school an e-Safety Policy that complies with education guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Group is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. Students, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, Students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from Child Exploitation and Online Protection (CEOP), Childnet, and UK Council for Child Internet Safety (UKCCIS) been obtained?	Y/N
Is e-Safety training provided for all Students (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all Students?	Y/N
Do parents/carers or Students sign an Acceptable Use Policy?	Y/N
Are staff, Students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by TB?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by DJB?	Y/N

Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member Senior Leadership Team (SLT) (currently DJB)	Y/N
Does the school log and record all e-Safety incidents, including any action taken? MG	Y/N
Are the Governing Body and SLG monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	Y/N

21. e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Additional Reading

http://www.bristol.gov.uk/sites/default/files/documents/children_and_young_people/child_health_and_welfare/BSCB%20Annual%20Report%202012-13%20%5BFINAL%5D%20V1_08.pdf

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis