Date: December 2021
Review date: December 2022
Responsibility: KB

Bishop Challoner School

E-Safety Policy

Bishop Challoner School
E-Safety Policy

This E-safety policy outlined below applies to all members of the school community including staff, students/pupils, volunteers, parents/carers, and visitors. It applies to the whole school, including the Early Years Foundation Stage.

Overview

In delivering the curriculum, teachers need to be able to incorporate communication technology including web-based resources, e-mail and mobile technology into their lessons.

There are a number of benefits and risks of using technology and the e-safety policy, safeguards and provides awareness for users to enable them to control their online experience.

The e-safety policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole and has been written by the school, building on the Kent e-safety policy and government guidance issued September 2020.

The school's e-safety policy will operate in conjunction with other policies including those for safeguarding, ICT, behaviour management, ICT code of conduct, anti-bullying, social media, curriculum, child protection, data protection and security.

It is important that the school and parents provide suitable strategies for the safe and effective use of the internet. A whole school approach to online safety is encouraged as this is more effective than lessons alone. Such an approach goes beyond teaching to include all aspects of school life including culture, ethos, environment and partnerships with family and the community.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils 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.

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.

From September 2020 RSE will be compulsory for all secondary aged pupils and through this new subject pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.

Roles and Responsibilities

The Designated Safeguarding Lead and IT Support have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Partnership. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Bishop Challoner believes that it is essential for parents / carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents / carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

Staff Awareness

New staff receive information on Bishop Challoner's e-Safety and Acceptable Use policies as part of their induction. All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.
All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Safeguarding Lead.

Teaching and Learning

The importance of the Internet and Digital Communications

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils so that they can learn how to locate, retrieve and exchange information and take care of their own safety and security. We therefore have a duty to provide quality internet access as part of the learning experience.

Enhance and Extend Learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils are given internet safety lessons from foundation stage to year 6. This covers social media sites, cyberbullying, emailing and chatrooms. We also discuss plagiarism and how to research safely.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils and staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Remote/blended Learning

During periods of remote learning following a full or partial school closure, Microsoft SharePoint and Teams may be used to deliver lessons and share resources. Pupils in the Junior school may also have access to Purple Mash.
Staff and pupils may only use their school email accounts to communicate and online contact should be restricted to school hours.
Online lessons will be formally timetabled and all participants must be informed if the session is being recorded. The use of video cameras maybe permitted, however, all participants must ensure they are appropriately dressed and have neutral backgrounds.
Appropriate privacy and safety settings will be used to manage access and interactions. Only members of staff can mute or disable participants' videos and microphones. Any chat facility should be used for learning purposes only and not social interactions between pupils.
Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
All participants are expected to behave in line with existing policies and expectations. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the appropriate Head of Section or Deputy Head.
Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.
Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.

Evaluation of internet content

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Pupils are asked to consider the following:

- Is the website/email fake? Check the address
- What information am I sharing?
- Why does someone want me to see this?
- Why does this person want my personal information?
- Is this too good to be true?
- Is this fact or opinion?

Under the Counter Terrorism and Securities Act 2015 schools are required to ensure that children are safe from terrorist and extremist material on the internet.

Pupils 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.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Network Manager or the Designated Safeguarding Lead.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.
Virus protection will be updated regularly.
Servers, wireless systems and cabling are securely located and physical access restricted.

All users (at KS2 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password.
Age specific advice on potential harms and risks can be found at:
https://www.gov.uk/government/publications/education-for-a-connected-world

E-mail *(This does not apply to EYFS pupils who do not have access to school e-mail accounts) However, Foundations stage are taught how to use a simple email package using a safe school-based software called 2email. This shows the principal rules of emailing.*
Pupils may only use approved e-mail accounts on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
The forwarding of chain letters is not permitted.
Electronic communication between school staff and its pupils must be through school e mail only.

Published content and the school Website

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The school's website editor will take overall editorial responsibility and ensure that content is accurate and appropriate.

Safe use of digital and video images

All pupils (or parents' of pupils aged under 13) are asked to complete the GDPR Media Consent form which gives details of where consent has been given for photographs may be displayed.

Photographs that include pupils will be selected sensitively according to the context in which they are used. Unless consent has been granted, pupils' full names will not be used anywhere on the public website, particularly in association with photographs.

All users should be aware of the potential risks of using social media. However, social networking sites can be a very useful educational tool and may be used to embrace learning outside the classroom.
The school will block/filter access to social networking sites for pupils using the school's internet service. Newsgroups will be blocked for pupils unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that the use of social network sites outside school have age restrictions and user agreements and are inappropriate for primary aged pupils.

Staff must be vigilant of the potential risks in communicating in a way which can be seen easily by parents or pupils. Such communications must be professional and do nothing to harm the reputation of the school or a member of staff. Users must not add comments or photographs which may bring the school, themselves or others into disrepute.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming 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.

When using digital images, staff should inform and educate pupils 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).

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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images must not be published on blogs or social networking sites (etc.), nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the ICT Acceptable Use Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Managing filtering

Technical support staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
If staff or pupils discover an unsuitable site, it must be reported to the Network Manager.

Managing Cloud based storage and use

No data containing information about pupils, their personal details, report data, exam results, or any other data of a sensitive nature should be stored on a Cloud based storage system with the exception of our MIS System. This also applies to data containing information about staff. Please refer to the ICT Acceptable Use Agreement under Information Security.

Managing video conferencing/skyping

Pupils should ask permission from the supervising teacher before making or answering a videoconference call or skype. Videoconferencing or skyping will be appropriately supervised for the pupils' age.

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.
Mobile phones will not be used during lessons or formal school time, unless specifically directed by a member of staff to do so. The sending of abusive or inappropriate text messages is forbidden.

Staff are asked not to make personal calls during their working hours.

Staff **must** use a school phone number where contact with pupils is required. There are school mobile phones for use during trips, visits and fixtures etc. **Personal telephone numbers may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number.**

In the EYFS, mobile phones may not be taken into the classroom, toilet and changing areas or used in the presence of the pupils for any purposes. Many mobile phones have inbuilt cameras so these staff mobile phones should be left with personal belongings in a secure area.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

Policy Decisions

Authorising Internet access

All staff and pupils must read and sign the 'ICT Acceptable Use Agreement' (AUA) before using any school ICT resource.

Expectations are set out in detail in the Acceptable Use Agreement and in the Social Media Policy, but include:

- Keeping a proper professional distance e. g. not "friending" pupils on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or e-mails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents.

In the EYFS and the Junior School parents are asked to read the 'Pupil Acceptable Use Agreement and e Safety Rules' with their child and sign on their behalf. Parents of junior and senior school pupils will be asked to counter sign the "Pupil Acceptable Use Agreement and e Safety Rules" and return to school.

The school maintains a record of all staff/adults and students who are granted access to School ICT systems. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

Misuse of school systems

Because the staff Acceptable Use Agreement is part of the contract of employment, misuse is a disciplinary matter.

Pupil misuse (for example the sending of bullying messages to another pupil) may result in the withdrawal of facilities or further sanctions in line with the school's disciplinary policy.

Abuse of the systems by visitors will result in the immediate withdrawal of access and possible further action depending on the nature of the misuse.

Handling e-safety complaints

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Parents and pupils will need to work in partnership with staff to resolve issues.

Particular concerns:

Inappropriate material appearing on school computers.

Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting.
They are encouraged to talk to their teacher.
The teacher should report the incident to the DSL who will log the problem and liaise with the network manager to adjust filtering settings.

Abusive messages on school computers

Pupils who receive abusive messages over school systems will be supported, and advised not to delete messages.
The DSL will be informed and an investigation begun initially with the help ofthe Network Manager.

Parental reporting of bullying/pressure.

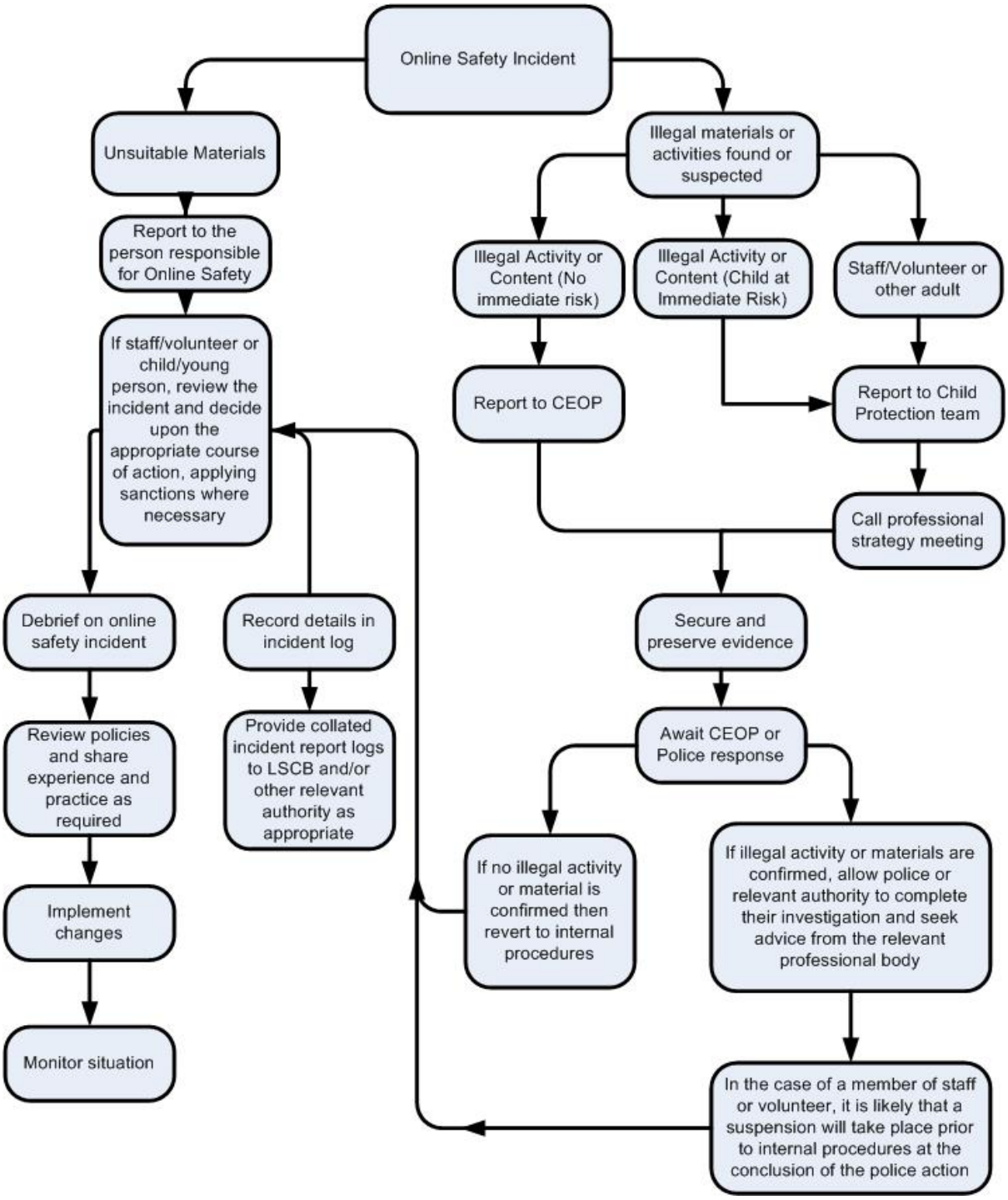
Parents may become aware that their child is suffering from bullying or other pressures origination in the school but continue via electronic means.
Parents should know that the school encourages parents and pupils to approach them for help, either via the class tutor or directly to the Headteacher.
A full discussion of Cyber bullying, and the actions which may be taken can be found in the Anti-Bullying and Cyber Bullying policies.

Pupil disclosure of concerns or abuse

For many reasons, a pupil may choose to disclose a concern to a member of school staff. The situations leading to a disclosure can range widely, from a general worry to long term abuse, and for this reason safeguarding training for all staff is conducted so that situations or concerns are dealt with appropriately
A disclosure should always be passed on to the Designated Safeguarding Lead

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.



Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms with internet access and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored.

Staff and the e-safety policy

All staff will be given the school e-safety policy and its importance explained. Training in safe and responsible internet use and on the school e-safety policy will be provided as required.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Using non-School Equipment

Under some circumstances, teachers and pupils in the sixth form are able to use their own equipment in school and connect to the available Wi-Fi.

This is normally called "bring your own device" (BYOD). Currently approved Device Types are: Smartphone's, Tablet Computers, Laptops, iPads only.

It is not the schools responsibility to provide or support personal devices. The purchase, maintenance, safety, insurance and security of all personal devices must be borne by the parents/pupils/staff.

The use of personal ICT devices falls under Bishop Challoner School's ICT Acceptable Use Agreement Policy which all students/staff must agree to, and comply with.

Whether staff member or pupil, it is made clear to the user that the rules and expectationssurrounding online beh aviour remain in force regardless of the ownership of the equipment being used.
Students are not permitted to connect to any external wireless or networking service (e.g. 3G/GPRS etc.) while using a personal ICT device in school.

Pupils and staff must check their personal ICT device daily to ensure the device is charged, free from unsuitable material and free from viruses etc. before bringing the device into school. Any personal ICT device that has obvious Health and Safety defects should not be brought into school.

Under no circumstances are pupils/staff permitted to bring into school or use privately owned chargers for personal devices.

Bishop Challoner School accepts no liability in respect of any loss/damage to personal ICT devices while at school, during school-sponsored activities or in transit. Only portable charging devices are allowed or charged via a plug socket. Any devices using plug sockets must be PAT tested.

As BYOD is not compulsory, the decision to bring a personal ICT devices into school rests with the student (and their parent(s)/guardian(s)) and staff as does the liability for any loss/damage that may result from the use of a personal ICT device in school.

When accessed from personal devices on / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

Enlisting parents' support

Parents' attention will be drawn to the school e-safety policy in newsletters and on the school website.

The school will support parents' understanding of e-safety issues in the home through information evenings and assemblies.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Vulnerable pupils

Any pupil can be vulnerable online and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, e.g. looked after children and those with SEND, who may be more susceptible to online harm or have less support from family or friends in staying safe online. The school will therefore consider how to ensure these pupils receive the information and support they need.
Further information can be found at: https://www.internetmatters.org/about-us/vulnerable-children-in-a-digital-world-report/

Information and support

There is a wealth of information available to support schools to keep children safe online. The following is not exhaustive but should provide a useful starting point: www.thinkuknow.co.uk
www.ceop.police.uk/safety-centre/
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
www.educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
www.gov.uk/government/publications/education-for-a-connected-world
www.gov.uk/government/publications/keeping-children-safe-in-education--2

K Brooker
Reviewed: December 2021
Review date: December 2022