Policy:	E-safety and acceptable use policy
Approval:	Headteacher
Date:	November 2024
Next review:	Autumn 2025

CHELTENHAM BOURNSIDE SCHOOL

Policies

Contents

1. Scope 3
3. Guidance for all Users 3
4. Guidance for Staff 4
5. Guidance for Students 5
6. Guidance for Parents 5
7. Student use of Mobile Technology 6
8. Digital Images and Photography 6
9. Policy Statements 6
10. Technical Infrastructure/Equipment, Filtering and Monitoring 7
11. Responding to Incidents of Misuse 7
12. Removal of Access to IT Systems 8
13. IT Support Requests and Change Management 8
14. Other Related Policies 9

1. Scope

This policy applies to staff, students, governors, parents/carers and visitors who are referred to as ‘users’. The policy covers the use of IT systems both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other e-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 the deletion of data on electronic devices.

2. Roles and Responsibilities

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the appropriate pastoral staff.
- The Senior Leader with oversight of Information Technology (IT) has a leading role in establishing and reviewing the school e-safety & acceptable use policy, procedures & documents.
- The Senior Leader with oversight of continuous professional development (CPD) is responsible for ensuring that staff receive suitable training with regards to the content of this policy.

Pastoral Staff and Designated Safeguard Lead (SL)

- Head of Houses, the Designated Safeguard Lead (DSL) and House Welfare Leads take day to day responsibility for E-safety issues.
- Have awareness of inappropriate on-line contact and the potential for grooming, cyberbullying, radicalisation and other malicious, criminal, abusive or inappropriate online behaviour.

Senior IT Manager and IT Services Team

- Responsible for ensuring that the school’s IT infrastructure and systems are secure and are not open to misuse or malicious attacks.
- Users may only access IT resources using unique IDs, secured by passwords or other suitable means.
- Access to the Internet is appropriately filtered and logged, and the implementation of the filtering system is not the sole responsibility of any single person.
- The elevated levels of access that they are granted as system administrators are used in accordance with this policy.
- New staff confirm they have read this policy by email or online data collection.

3. Guidance for all Users

- All users should ensure that they have an up-to-date knowledge of this policy and an awareness of E-Safety matters.
- All users should keep their credentials for accessing school IT systems secure and should not share these. If users suspect their password has been compromised, they should change it immediately.
- All internet access is filtered and monitored.
- Personal devices brought into school must not introduce vulnerabilities into existing secure environments.
- Users shall not visit internet sites, that relate to:
    - Child abuse images
    - Pornography, violence, intolerance, self-harm, profanity, gambling or weapons
    - Illegal software, drugs or substance abuse
    - 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.

- Illegal or unacceptable content is filtered by the broadband or filtering provider by actively employing theInternet Watch Foundation CAIC list, or similar by the school internet service provider.
- Users should not open any hyperlinks in emails or any attachments unless they know and trust the sender.
- Users should not use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Any potential security breaches should be reported to a member of staff.
- Users should adhere to copyright guidelines.
- Personal devices should not be plugged into electrical sockets in school.
- The school may monitor the use of systems, devices and digital communications.
- Users must immediately report to a teacher, line manager, or member of the Senior Leadership Team, 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.
- Users should not engage in online discussion on personal matters relating to members of the school community.

4. Guidance for Staff

- Teaching staff should ensure that key messages outlined in this policy are communicated to students when using the school's IT systems.
- Staff should keep devices secured such that students, parents and guests cannot gain access to personal data. This includes not allowing students to use staff credentials and ensuring that computers are signed out of or locked when not being used.
- Access to core systems such as staff email, and the school's MIS must be protected by multi-factor authentication.
- Personal data must not be sent over the internet unless appropriately encrypted.
- All digital communications between staff, students and parents/carers must be professional in tone and content.
- All recorded comments about students, parents or staff on school systems must be professional in tone and content, such that it could be shared with the relevant stakeholder if requested.
- Users should not use school systems to run a private business.
- No reference should be made in publicly accessible social media to students, parents/carers or school staff other than for reporting school news via the official school website and social networking accounts.

- Such social networking accounts should only be created in consultation with the school's Marketing and Communications Manager.
- Staff must not 'befriend' students or parents/carers on social networking and maintain a 'professional distance'. Where there may be an exception to this granted for students or parents/carers that are family members or close friends, this should be brought to the attention of the Headteacher.
- Staff are only permitted to use personal email and social networking at work at the Headteacher's discretion. Without this discretion, practice should be that this is only done outside of directed time (for teaching staff) or normal working hours (for support staff); staff may, therefore, use personal email and social networking discretely during their unpaid breaks.
- Staff should report any potential security breaches or suspected misuse of IT to the Senior IT Manager or DSL as appropriate.
- All staff must undertake Cyber Security training provided by the NCSC: Cyber security training for school staff - NCSC.GOV.UK

5. Guidance for Students

- Students must not take, use, share, publish or distribute images of others without their permission.
- School systems and devices are primarily intended for educational use. Students are not permitted to use them for personal or recreational use.
- Students should report any damage or faults involving equipment or software.
- Students must not attempt to install software of any type on any school device.
- Students must be polite and responsible when communicating with others and not use inappropriate language.
- Students must not set up social media platforms or groups that use the school name or logo.
- Students must not engage in cyber-bullying, including sending inappropriate text messages or posts on social media that are likely to offend or upset others.
- Personal information should not be disclosed when on-line.
- Students are discouraged from arranging to meet people that they have communicated with online and are always to do so in a public place and to take an adult with them.
- You should immediately report any unpleasant or inappropriate material when you see it online.

6. Guidance for Parents

- Parents/carers are encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:
    - Digital and video images taken at school events.
    - Access to student records through the school's electronic systems.
    - Their children's personal devices in the school.

- 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. To respect everyone's privacy and in some cases protection, these images must not be published or made publicly available on social networking sites.
- Parents/carers are politely asked not to discuss school matters or issues related to Cheltenham Bournside School on social media. Any concerns that need discussing

should be raised directly with the school.
- Parents may add their child to the 'no photograph' list by indicating this on the student data collection form sent to parents.

7. Student use of Mobile Technology (iPads, tablets, mobile phones and / or similar devices as well as headphones)

- We recognise that schools are places where students learn social skills through face-to-face conversations. Because of this, students are not permitted to use their phones at any time; the only exception to this is use of mobile phones as cameras as part of the GCSE or A'level Photography courses. The use of mobile technology outside of lesson time and/or without the permission of the teacher is prohibited on the school grounds and will result in the following disciplinary sanction:
    - First occasion – mobile technology confiscated. Student can collect from student reception at the end of the school day.
    - Second occasion – parents/carers will be required to collect the mobile technology from reception and whole school detention will be issued.
- If a student refuses to hand over the mobile technology at the request of a member of staff, then a Level 3 sanction will be applied that is a fixed term of 1 day in the BRC, this includes a whole school detention.
- If a student refuses to hand over their mobile technology to a member of SLT, they will incur a suspension from school.
- Confiscated mobile technology should be passed to Reception by 3:15pm on the day of confiscation.

8. Digital Images and Photography

- Staff and governors are allowed to take digital/video images to support educational aims but must check that pupils being photographed are not on the 'no photograph' list.
- Published photographs should not identify the full name of the student.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the school website, or social media platforms that include students will be selected carefully and will comply with good practice guidance on the use of such images. They will not be published together with the full name of the child.
- Students' full names will only be used on blogs and social networking when there is no accompanying photograph, including group photographs.

9. Policy Statements

The education of students in e-safety is an essential part of the curriculum. We recognise that children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. The school has a planned e-safety curriculum including:

- A 10-week project in Year 7 focused on cyber-bullying
- Year 7 - Education for Life lessons on e-safety, building online relationships
- Year 8 - Sexting and online safety revisited
- Year 9 - Employability and your online presence and online grooming

- Year 10 - Online gambling, pornography
- A 10-week project in Year 9 focused on protecting their digital identity and footprint
- Key e-safety messages are reinforced in assemblies to all year groups.
- Students are taught in all relevant lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information as appropriate. This also includes how to evaluate what they see online, how to recognise techniques used for persuasion, online behaviour, how to identify online risks and how and when to seek support.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet as appropriate to their studies.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit; reporting any inappropriate sites found to IT Services.

10. Technical Infrastructure/Equipment, Filtering and Monitoring

School IT systems are managed in ways that ensure that the school meets recommended technical requirements for e-safety.

- There are regular reviews of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted as appropriate.
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with unique credentials by IT Services.
- Administrator passwords for school IT systems, are available to the Headteacher or other nominated senior leader with responsibility for IT.
- Data is stored securely and backed up to a separate location to minimize data loss in the event of a disaster recovery scenario.
- The Senior IT Manager is responsible for ensuring that software licenses are valid and up to date for the required number of installations or users.
- Appropriate security measures are in place to protect the school's IT infrastructure from accidental or malicious attempts which might threaten the security of the school systems and data.

11. Responding to Incidents of Misuse

If there is any suspicion that the activity concerned may contain child abuse images, or if there is any other suspected illegal activity, the matter will be reported to the police. The person responsible for Online Safety in this context is the Headteacher.

12. Removal of Access to IT Systems

The school's HR team will notify IT Services when a member of staff's employment terminates, so that their access to IT systems can be removed accordingly. The admissions team will advise of any students who are taken off roll.

Individual heads of department or team leaders must ensure that access to any shared document libraries or email accounts that they oversee are kept current. This may involve removing access for a member of staff who leaves their team or department, or instructing IT Services to make the necessary changes on their behalf.

13. IT Support Requests and Change Management

Requests for IT technical support should be submitted by email wherever possible, to itservices@bournside.gloucs.sch.uk

Requests that require changes to school devices, configuration or infrastructure will be reviewed and processed as follows:

- Requests that require changes to be made that are restricted to an individual person or device will be assessed and implemented appropriately by a member of the IT Services team.
- Requests that require wider changes to the configuration of the school's infrastructure or systems will be passed on to the Senior IT Manager or appropriate deputising member of staff for approval before being scheduled for action.
- Requests that will result in a change to the way in which the school functions, or that conflict with existing policy or procedure will be passed on to the Senior IT Manager for technical assessment. Consultation with the Senior Leadership Team will then take place before final approval.

14. Other Related Policies

- Keeping Children Safe in Education (DfE, September 2019)
- Teaching Online Safety in School (DfE, June 2019)
- Behaviour Policy
- Anti-bullying Policy
- Safeguarding and Child Protection Policy
- Data Protection Policy.