Policy:	E-safety and acceptable use policy
Approval:	Headteacher
Date:	January 2026
Next review:	Spring 2027

CHELTENHAM BOURNSIDE SCHOOL

Policies

Contents

Revision History

Date	Version	Changes made	Approved by
21.10.25	8	Section 3 – Guidance for all Users Section 4 – Guidance for Staff Section 7	Mr Jefferies
30.01.26	9	Appendix	Mr Jefferies

1. Scope

This policy applies to staff, students, governors, parents/carers and visitors who are referredto 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 ofthis policy.

Pastoral Staff and Designated Safeguard Lead (SL)

- Head of Houses, the Designated Safeguard Lead (DSL) and House Welfare Leads takeday 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 andare 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 that they have read this policy and completed the mandatory NCSC Cyber Security Training 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, theyshould change it immediately.
- All internet access is filtered and monitored.
- Personal devices brought into school must not introduce vulnerabilities into existingsecure environments.
- The use of removable media is only permitted where appropriate encryption is enabled on the device.
- 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 theintegrity 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.
- The school's web filtering and monitoring system is subject to SSL inspection. This means it is theoretically possible for our internet service provider to view data that is sent and received via our broadband connection.
- Users should not open any hyperlinks in emails or any attachments unless they knowand trust the sender.
- Users should not use systems, applications, websites or other mechanisms that bypassthe 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.
- 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 notrespond to any such communication.
- Users should not engage in online discussion on personal matters relating to membersof the school community.

4. Guidance for Staff

- Teaching staff should ensure that key messages outlined in this policy arecommunicated 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 schoolwebsite 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 supportstaff); staff may, therefore, use personal email and social networking discretely duringtheir unpaid breaks.
- Staff should report any potential security breaches or suspected misuse of IT to theSenior 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 before being granted access to school IT systems.

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 orlogo.
- Students must not engage in cyber-bullying, including sending inappropriate textmessages 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 communicatedwith 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-Safetypractice 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/carersare 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 studentdata

collection form sent to parents.

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

- For KS3 and 4, the use of mobile phones on school site is prohibited at all times. This means that mobile phones cannot be used for any reason from the moment students arrive on the school site and until they leave the school site at the end of the school day.
- Mobile phones must be always switched off and in school rucksacks/bags throughout the school day. If a student does not bring a bag/rucksack to school they cannot bring a mobile phone. From January 1 2026, they will also need to be in a locked "Focus" pouch.
- If a mobile phone is anywhere other than in the student's rucksack/bag and/or is not switched off this will result in the following disciplinary sanction:
    - On every occasion – device confiscated, handed to reception and a whole school detention will be set. Parents/carers will be required to collect the device from reception by 4:30pm Mon-Thurs and 4:00pm on a Friday (if the parent/carer cannot collect the device it will be stored securely by the school until such time it is collected by the parent/carer).
- Persistent breaches of the mobile technology expectations will incur a higher sanction including handing the mobile phone to the respective Head of House for the duration of the school day. The number of days of this sanction period will be at the discretion of the Head of House.
- These rules also apply to Sixth Form students except when being used in the sixth form study areas. Any confiscated devices in sixth form should be handed to the sixth form office.
- Students whose My Profile or My Plan specifically states that they require the use of mobile technology as a support strategy may use their phones or tablets during the school day.
- This section of the policy will be amended from January 2026; from that point, the approach to mobile phone use described in the School's behaviour policy will apply and will supersede this section of this policy.

8. Digital Images and Photography

- Staff and governors are allowed to take digital/video images to support educational aimsbut 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. Responsible use of AI

- AI technologies must never be used to process personal or sensitive data about students, parents or staff, as this may result in a serious data breach.
- The following tools are examples of known "AI technologies" used across the school:
    - ChatGPT
    - Microsoft CoPilot
    - Google Bard
    - Canva

      (note this is not an exhaustive list).
- If you are unsure whether software being used is considered "AI technology", you should

consult with IT Services for clarification.

- Many AI technologies have strict age restrictions and must only be used in age appropriate contexts and with proper supervision.
- Before using any new AI technology, you should consult with the IT team to ensure a Data Impact Assessment is completed and seek approval from your SLT link.
- Misuse of AI technologies could expose the school to legal and reputational risk, which staff are responsible for helping to prevent.
- AI generated content must not be used in any way as part of your work, unless you have checked it for accuracy and appropriateness.

10. 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.

11. Technical Infrastructure/Equipment, Filtering and Monitoring

School IT systems are managed in ways that ensure that the school meets recommendedtechnical 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 accessrestricted 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 andup 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.

12. Responding to Incidents of Misuse

If there is any suspicion that the activity concerned may contain child abuse images, or ifthere 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.

13. 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.

14. IT Support Requests and Change Management

Requests for IT technical support should be submitted by email wherever possible, to [redacted]

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

- Requests that require changes to be made that are restricted to an individual person ordevice will be assessed and implemented appropriately by a member of the IT Servicesteam.
- 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.

15. Other Related Policies

- Keeping Children Safe in Education (DfE, September 2025)
- Teaching Online Safety in School (DfE, January 2023)
- Behaviour Policy
- Child Protection and Safeguarding Policy
- Data Protection Policy

Appendix: Artificial Intelligence (AI) Policy

Purpose

The purpose of this policy is to ensure that AI is used in a responsible and ethical way within Cheltenham Bournside School. It aims to ensure that the application of AI is in accordance with GDPR regulations cyber security best practices.

Scope

The policy applies to all staff, and students of Cheltenham Bournside School, as well as anyone who is using AI tools or systems on behalf of the organisation.

The following tools are examples of known "AI technologies" used across the school:

- Microsoft CoPilot
- ChatGPT
- Canva

If a member of staff is unsure whether the software they are using is considered "AI technology", they should consult with IT Services for clarification. Before using any new AI technology, staff should consult with IT Services to ensure that a Data Impact Assessment is completed and seek approval from the relevant SLT link.

Acceptable Use

AI tools may be used to improve efficiency, automate tasks and to support decision making. Their use in such contexts are encouraged, and practical examples include:

Automatically transcribing meeting notes
Summarising documents into key bullet points
Reducing repetitive tasks
Handling routine queries efficiently
Identifying trends and insights for better decision making

Prohibited Use

The misuse of AI technologies could expose the school to legal and reputational risk. As such, they must not be used for any unlawful, discriminatory or harmful purposes. They must not be used in a way that may result in the generation of misleading or inaccurate content.

Staff should not use AI generated content in any way as part of their work, without checking it for accuracy and appropriateness.

AI technologies mustn’t be used to process personal or sensitive data in a way that could result in a data breach.