



ICT Pupil Policy (CC)

Digital Health & Safety and ICT Acceptable Use Policy: (inc Mobile Phones and other Electronic Devices). Information for parents.

For the purposes of clarity the following terms will be used throughout the policy:-
'Cheltenham College' refers to Cheltenham College Senior School and Cheltenham College Preparatory School (including Cheltenham College Nursery School)
'College' refers to Cheltenham College Senior School
'Cheltenham Prep' refers to Cheltenham College Preparatory School
'Kingfishers' refers to Cheltenham College Nursery School / EYFS

1. Purpose

- 1.1 Cheltenham College aims to
 - ensure secure and supervised access to information and communication technology (ICT) for all pupils
 - encourage pupils to use technology to support their learning
 - promote the notion of Digital Health and Safety
 - encourage all members of Cheltenham College community to gain a healthy balance of ICT use in both Cheltenham College and at home.
- 1.2 This policy supports these aims by describing Cheltenham College ICT-related practices as well as the expected behaviour of pupils when it comes to using ICT whilst in the care of Cheltenham College.
- 1.3 This policy applies to the use of internet and electronic mail facilities, file-servers, messaging services, and any networks or hardware, including, but not limited to, those provided by Cheltenham College.
- 1.4 It applies to any personal devices including computers, mobile phones, audio players, cameras and any other equipment that can be used to access, store, transmit or record data or media files.

2. Devices

- 2.1 All College pupils are required to have a suitable laptop device at College.

- 2.2 Cheltenham College will provide a number of software packages for pupils for teaching and learning, personal administration, communication and security and all devices must be compatible with these packages in order to connect to Cheltenham College network. (Compatible device options are provided via the Purchasing Portal)
- 2.3 College provided software must not be tampered with or removed.
- 2.4 Pupils at The Prep are not permitted to bring in their own equipment except by arrangement with the SENCo or as part of agreed measure of learning support put in place by College.

3. Network Access

- 3.1 Pupils must only access Cheltenham College systems and the internet via the 'Cheltenham College' WiFi network.
- 3.2 Pupils should not access the Internet via their mobile data networks (e.g. dongles or smartphone 'personal hotspots'), commercial WiFi hotspots (e.g. BT) or via public WiFi networks such as those provided by hotels and cafes.
- 3.3 Personal devices such as phones may be connected to Cheltenham College WiFi network but priority will be given to the quality of service for laptop devices, as the primary means of supporting teaching and learning delivery.

4. Acceptable Use

- 4.1 Pupils must not gain or attempt to gain unauthorised access to Cheltenham College or other people's devices, facilities, data, or services.
- 4.2 Pupils must not interfere with the work of others or the system itself.
- 4.3 Pupils must not attempt to bypass any service restrictions or security controls placed on the network by Cheltenham College (or its agents).
- 4.4 Pupils must not create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person.
- 4.5 Pupils must not transmit any messages pretending to be someone else e.g. by using their accounts without permission.
- 4.6 Pupils must not send any communications internally or externally that is bullying, abusive, humiliating, hostile or intimidating.
- 4.7 Pupils must not send messages to more than 20 recipients without the approval of a member of the ICT department.
- 4.8 Pupils must compose any email (or other electronic communication) with courtesy and consideration.

5. Access Restrictions

- 5.1 Pupils' access to the Internet is scheduled at College. The current schedule of access times is posted in each of the boarding houses.

- 5.2 Access to inappropriate or offensive websites is blocked from Cheltenham College networks and varies depending on the age of the pupil.

6. Physical Protection

- 6.1 Pupils should always look after their devices. There are secure, lockable storage facilities in Houses for the storage of pupils' laptops.
- 6.2 Pupils must take sensible precautions to avoid computer viruses.
- 6.3 Should pupils believe their device may be infected they should arrange to have it checked as soon as possible.

7. Login Security

- 7.1 Pupils must not disclose passwords to anyone and must not attempt to discover or use the passwords of others.
- 7.2 Should pupils believe the security of their passwords has been compromised they must arrange to have their password reset immediately.
- 7.3 College passwords should be different from non-College passwords.

8. Confidentiality

- 8.1 Any College information or records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless Cheltenham College's prior written consent has been obtained.
- 8.2 This requirement exists both during and after a pupil's time at Cheltenham College. In particular, pupils or ex-pupils must not use such information for the benefit of any future employer.

9. Overnight Arrangements

- 9.1 Internet-enabled devices belonging to Lower College pupils will be collected overnight and stored securely by House staff, in order to ensure that pupils are not distracted from sleep.

10. Social Networking

- 10.1 The use of social networking sites can be a particular concern for parents and College alike. Cheltenham College therefore limits and monitors pupils' access to such sites during term time. It also supports and educates pupils and parents in social networking as part of its Digital Health programme.
- 10.2 Pupils must not access any social network sites, through whatever means, outside of the controlled access times.
- 10.3 Prefects are expected to inform the Housemaster / Housemistress (HsM) if Lower College pupils are caught using social media outside of the controlled times.
- 10.4 Pupils at The Prep are not permitted to access any social networking sites through the school's computers.

11 Gaming, Streaming and DVD

- 11.1 Issues relating to gaming and the watching of DVDs or streaming services (including access to sites like Netflix or Amazon Prime and relating to all 'streaming' or online activities), focus around
- The negative impact on work and study ethic
 - Access to only age appropriate games and films
 - Their addictive nature
 - The illegal copying/streaming of games/other copyright material
 - The impact on the network access/traffic speed available to other when such media are used
 - The anger and frustration games can evoke in some pupils
- 11.2 Cheltenham College therefore only permits boarders to play games and to watch films from 4.00 pm on Saturday to 6.00 pm on Sunday.
- 11.3 Games and DVDs may be allowed at prep break at the HsM's discretion.
- 11.4 Pupils must not play games or watch films, through whatever means, outside of the permitted hours.
- 11.5 Pupils must only watch and play games that are age appropriate. Any material that is not age appropriate will be confiscated and will be returned to parents at the next opportunity.
- 11.6 Pupils at The Prep are not permitted to play on games or watch films on the school's computers that are not age appropriate.

12. Cyber bullying

- 12.1 Cheltenham College's preventative measures and procedures for dealing with Cyber bullying are found in Cheltenham College and Prep Anti-Bullying Policies (Refs 1&2).
- 12.2 Pupils must be clear that the online College community exists both during and outside of term time.
- 12.3 There will, therefore, be circumstances in which inappropriate online behaviour will be dealt with as a school issue, even if it occurs during the holidays. These would typically include any behaviour that could bring College into disrepute or which has a serious impact on Cheltenham College community or individuals within it.
- 12.4 Further details are contained in Cheltenham College's Behaviour Policy (Ref 3).

13. Sexting

- 13.1 Pupils must be especially aware of the dangers of sexting. It is illegal to be in possession of, or to transmit, an inappropriate image of a person under the age of 18 (even if sent with their consent). Under Cheltenham College's Behaviour Policy (Ref 3), requesting such Images is a very serious matter as most young people (boys and girls) experience such requests as a form of bullying.
- 13.2 Should a pupil receive an inappropriate image they should immediately advise a member of staff, usually the relevant HsM, and then delete the image under supervision.

13.3 At The Prep, pupils can forward any inappropriate messages or material to safe@cheltenhamcollege.org

14. Privacy and Reputation

14.1 No one should put anything onto the web that they would not be prepared for parents, teachers etc to read. The web is a public forum. Any blog or photograph posted onto the Internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or Internet archive and cause embarrassment years later. Once images are forwarded to others, the same applies. The consequences of getting this wrong may result in a serious breach of College's Behaviour and Anti-Bullying Policies and in addition may have tragic personal consequences.

15 Mobile Phones

15.1 Cheltenham College wants to encourage pupils to use their mobile technology to support their learning, but pupils are required to follow the following guidelines

- Pupils must seek permission whenever they wish to use personal devices in lessons (and other College provided activities)
- Pupils must respect others' wishes not to be photographed or recorded
- Pupils must not film or record others without their knowledge and consent

15.2 Upper College students may use mobile phones in the Library if using headphones (only for the purposes of listening quietly to music) or in Social during the school day, but in no other places.

15.3 Lower College pupils should not be using mobile phones during the school day except with the express permission of a teacher.

15.4 Cheltenham College does not normally expect staff and pupils to communicate with each other by mobile phone. This is permitted in some exceptional circumstances, such as on trips and outings.

15.5 The exception to this is the use of emergency mobile phones by House staff.

15.6 Day pupils at The Prep are not permitted to bring mobile phones into school except by arrangement with the Deputy Head (Pastoral). Phones will be dropped off at Prep Reception in the morning and collected by the pupils on leaving the school at the end of the day.

15.7 Boarders have set times in the evening when they are allowed access to their mobile phones and devices. Each item is signed out and in by a member of staff and all devices are securely stored.

16 Cameras

16.1 Cameras, including those on mobile phones, must not be used in a way that could justifiably be regarded as intrusive or embarrassing.

16.2 Cameras, including those on mobile phones, are not permitted in lessons (except with express permission of the teacher for educational purposes), Chapel, plays, concerts or in any other College activity where they could justifiably be regarded as an interference, intrusion or breach of copyright.

- 16.3 Cameras, including those on mobile phones, may be used at matches and in houses.
- 16.4 Cameras, including those on mobile phones, must not be used in any changing or washing areas.
- 16.5 Staff and pupils must take particular care where cameras, including those on mobile phones, are taken into pupils' bedrooms or dormitories.
- 16.6 Staff may only take and use images of pupils for work purposes, with the pupil's knowledge and may only store these images in access controlled College storage facilities.
- 16.7 Cheltenham College maintains a record of which pupils have consented to their image being used for College purposes.

17. Monitoring

- 17.1 Cheltenham College reserves the right to monitor communications, general network usage and media/software on individual devices in order to
- Protect and safeguard pupils
 - Establish the existence of facts
 - Prevent or detect crime
 - Investigate or detect unauthorised, suspicious or inappropriate use of Cheltenham College's ICT systems
 - Ensure the effective operation of Cheltenham College network and its systems.

18 Device checks and searches

- 18.1 Cheltenham College reserves the right to perform checks on laptops, mobile phones and other personal devices for illicit activities or material. Cheltenham College may from time to time initiate random checks on pupil devices.
- 18.2 Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to
- cause harm
 - disrupt teaching
 - break school rules
 - commit an offence
 - cause personal injury, or
 - damage property.

Quarantine

- 18.3 There may be times when equipment is 'quarantined' by security systems in use at Cheltenham College. Should a pupil have trouble connecting from their equipment, they will be required to present at the IT office for this to be investigated.

Investigations

- 18.4 Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them.

- 18.5 Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy.
- 18.6 If the breach is of a criminal nature, the Police and Gloucestershire Safeguarding Children's Executive (GSCE) may be involved.
- 18.7 If Cheltenham College discovers that a child or young person is at risk as a consequence of online activity, it may also seek assistance from the Child Exploitation and Online Protection Unit (CEOP).
- 18.8 The Designated Safeguarding Lead (DSL), the Deputy Head Pastoral or Senior Deputy Head will be involved in all such situations.
- 18.9 Cheltenham College will, where necessary, recover deleted files and material from devices to assist in an investigation.

19 Sanctions

- 19.1 Appropriate sanctions are imposed in line with Cheltenham College's Rewards and Sanctions (Ref 4), Suspension and Exclusions (Ref 5) policies.
- 19.2 Sanctions may include
- The restriction of a pupil's access to Cheltenham College network in both House and College
 - The confiscation of any personal or shared devices being used to infringe these or any wider Cheltenham College rules, or
 - More serious sanctions including gating, suspension or expulsion
- 19.3 Cheltenham College reserves the right to use its discretion when applying sanctions and the seriousness of the offence will be considered carefully before making any decision.

20 Confiscation

- 20.1 As part of Cheltenham College's Child Protection and Safeguarding responsibilities it may be necessary on occasion to confiscate from any pupil while at Cheltenham College his or her computer, mobile telephone, audio player or any other device capable of digital recording. The confiscated items are inspected and returned as rapidly as reasonably practicable. If the items contain inappropriate material, that material is wiped from the item's memory.
- 20.2 Members of staff may confiscate mobile phones for inappropriate use, passing them to College Office, as soon as practicable, which will contact the relevant HsM. The HsM will decide on an appropriate sanction, which would typically be: keeping the mobile phone for 24 hours (first offence), 48 hours (second offence) or longer-term confiscation with the involvement of parents (third offence).

21 Support

- 21.1 Cheltenham College recognises that blocking and barring sites is no longer adequate, especially in an age when so many pupils have access to smart phones and dongles, which can bypass Cheltenham College network. It aims therefore to teach all pupils to understand why they need to behave responsibly if they are to protect themselves and avoid harm to others.

- 21.2 All staff, at both The Prep and Cheltenham College, are directly and actively involved in supporting Digital Health.
- 21.3 The Floreat programme is one of the primary means of supporting digital health in College pupils.
- 21.4 Pupils and parents alike can raise concerns with the Deputy Head of Wellbeing at both the Prep and College or with the relevant HsM.
- 21.5 Pupils in the Third Form are given a talk about ICT and this covers the use of social network sites as well as other digital health topics.
- 21.6 The Designated Safeguarding Lead (DSL) (Ref 6) has a responsibility to help understand and monitor digital health issues and assist in the education of pupils and staff on safe and responsible use of technology.

22. Working with parents and guardians

- 22.1 Cheltenham College sees to work closely with parents and guardians in promoting a culture of digital health and safety e.g. sunning information sessions for parents from time to time. This includes specialist advice about the potential hazards and practical steps parents can take to minimise potential dangers.
- 22.2 Cheltenham College will contact parents if there are serious worries about a pupil's behaviour and encourages parents to share any concerns of their own with Cheltenham College via the relevant HsM.
- 22.3 It is strongly recommended that smart phones should have the internet access via the mobile data network disabled or the data allowances restricted as such devices circumvent Cheltenham College network and make it far more difficult for Cheltenham College to keep pupils safe.
- 22.4 IT IS ALWAYS possible for pupils to have access to landline phones for contacting parents, or for other emergencies, by speaking to any member of staff, usually the HSM.

23 More information

- 23.1 Pupils and parents are encouraged to make use of the excellent online resources. A small number of which are summarised below.

bullying.co.uk

Part of Family Lives, a charity with over three decades of experience helping parents to deal with the changes that are a constant part of family life. In addition to a range of advice, provides a confidential helpline and forum.

childnet-int.org

Childnet International is a non-profit organisation working with others to help make the internet a great and safe place for children. The site provides advice for young people, teachers and professionals, parents and carers. Notably advice includes 'having a conversation' and detailed advice on a range of topics.

dove.com/uk/dove-self-esteem-project.html

The Dove Self-Esteem Project is an education initiative by Unilever, the makers of Dove products. It provides resources including parenting advice to help young people form healthy friendships, overcome body image issues and be their best selves.

mediasmart.uk.com/teaching-resources

Media Smart provides advertising, digital advertising, body image, and social media teaching resources for 7 – 16 year olds for parents, guardians and educators, so media and digital literacy can be taught more easily in school, and at home.

net-aware.org.uk

Net Aware is the O2 and NSPCC guide for parents to the most popular sites, apps and games that young people use. Parents can use the site to search for and learn whether an app, site or game is appropriate for their children in order to stay up to date in today's evolving digital world. Net Aware also provide an app version of the guide.

nspcc.org.uk

The National Society for the Prevention of Cruelty to Children is a charity campaigning and working in child protection in the United Kingdom and the Channel Islands. Its website provides some online safety advice alongside wider advice relating to preventing abuse. The NSPCC provide the Childline service.

parentinfo.org

Parent Info is a collaboration between Parent Zone and NCA-CEOP, providing support and guidance for parents from leading experts and organisations.

parentzone.org.uk

Parent Zone is both an expert consultancy in digital family life, responding to the global challenges of the digital age as well as a social enterprise that generates enough profit to run the operation, and the free services we offer parents, investing any surplus in projects that support families and parents.

pegi.info

The Pan-European Game Information (PEGI) age rating system was established to help European parents make informed decisions on buying computer games. Notably, it provides advice on the parental controls available within game consoles.

saferinternet.org.uk

A partnership of Childnet International, Internet Watch Foundation and Southwest Grid for Learning (SWGfL) that promotes the safe and responsible use of technology for young people. The partnership is one of 31 Safer Internet Centres appointed by the European Commission. It provides awareness advice for young people, parents and carers as well as schools and coordinates the UK Safer Internet Day. It provides a helpline to support to professionals and hotline to anonymously report child sexual abuse imagery.

thinkuknow.co.uk

Thinkuknow is the education programme from CEOP, a UK organisation which protects children both online and offline. The site provides advice about staying safe when you're on a phone, tablet or computer for both children at different ages and parents.

24 References

1. College Anti-Bullying Policy
2. Cheltenham Prep Anti-Bullying Policy
3. Cheltenham College Key Behaviour Policy
4. College and Cheltenham Prep Rewards and Sanctions Policies
5. Cheltenham College Exclusion Policy

6. Cheltenham College Key Child Protection and Safeguarding Policy

Reviewed: October 2021

Next review date: October 2022