



## **Cheltenham College**

### **Acceptable use of ICT, Mobile Phones and other Electronic Devices Policy**

#### **Introduction**

The College aims to ensure secure and supervised access to ICT for all pupils. This policy is intended to support this by outlining acceptable uses of ICT for pupils while they are in the care of the College. It applies to the use of internet and electronic mail facilities, file-servers, messaging services, and any networks or hardware, including but not limited to that provided by the College. It applies to any personal devices including, computers, mobile phones, MP3 players, cameras and any other equipment that can be used to access, store or record data or media files.

#### **Personal equipment**

All pupils have an Apple compatible laptop at College: any other personal equipment may only be directly connected with the agreement of the Network Director.

#### **Practice**

Pupils must not interfere with the work of others or the system itself. They 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. They must not transmit any messages or prepare files that appear to originate from anyone other than themselves. They must not gain or attempt to gain unauthorised access to other people's files or facilities or services accessible via local or national networks or transmit any confidential information about the College: they must not attempt to get around service limitations placed on network use by the College (or its agents). They must not send any message internally or externally which is bullying, abusive, humiliating, hostile or intimidating. They must not send messages to more than 20 recipients without the approval of a member of the ICT department. They must compose any e-mail (or other electronic communication) with courtesy and consideration.

#### **Security**

Pupils must not disclose passwords to anyone and must not attempt to discover or use the passwords of others. They must take sensible precautions to avoid Internet viruses.

#### **Confidentiality**

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 the College's prior written consent has been obtained. This requirement exists both during and after a pupil's time at the College. In particular, pupils or ex-pupils must not use such

information for the benefit of any future employer.

### **Monitoring**

The College reserves the right to monitor communications and general network usage in order to:

- Protect pupils
- Establish the existence of facts
- Prevent or detect crime
- Investigate or detect unauthorised, suspicious or inappropriate use of the College's ICT systems
- Ensure the effective operation of the College network and its systems.

### **Random checks**

The College reserves the right to perform random checks on laptops for illicit activities or material.

### **Sanctions**

In the event of any breach of the policy, appropriate sanctions are imposed in line with the College's behaviour and exclusions policy: this may include the restriction of a pupil's access to the College network, the confiscation of any personal or shared devices being used to infringe these or any wider College rules, or more serious sanctions including gating, suspension or expulsion. If the breach is of a criminal nature, the Police and Local Safeguarding Children's Board (LSCB) may be involved. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The Senior Designated Person (SDP) for child protection handles all such situations.

### **Confiscation**

As part of the College's Child Protection responsibilities it may be necessary on occasion to confiscate from any pupil while at the College his or her computer, mobile telephone, MP3 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.

### **Education**

The College recognises that blocking and barring sites is no longer adequate. It aims to teach all pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for the Director of ICT, who visits Houses giving talks to pupils, and the pastoral staff through the PSHCE programme. The College offers specific guidance on the safe use of social networking sites, which covers personal security settings.

### **Working with parents**

The College seeks to work closely with parents and guardians in promoting a culture

of e- safety, running evening information sessions on e-safety for parents from time to time. This includes specialist advice about the potential hazards and practical steps parents can take to minimize potential dangers. The College always contact parents if there are worries about a pupil's behaviour and encourages parents to share concerns with the College.

The use of social networking sites can be a particular concern for parents and College alike. The College has therefore introduced the following guidelines to limit, and monitor, pupils' access to such sites during term time:

The College limits access as follows:

- For Lower College:    Mon to Fri    8.45pm to 9.15pm  
                                  Weekend     1.00pm on Sat to 9.15pm on Sun
- For Upper College:    Mon to Fri    8.45pm – 10.30pm  
                                  Weekend     1.00pm on Sat to 10.30pm on Sun

Prefects also have a role to play in monitoring the use of Facebook and are expected to inform the HSM if Lower College are caught using it outside of the controlled times

Pupils should NOT come into College with mobile internet connectors e.g. 'dongles'. These will be taken from the pupils and returned at the end of half term/term. Smart phones should have the internet access disabled.

There will be secure, lockable storage facilities in Houses for HSMs to store pupils' laptops. Third and Fourth Form laptops will be stored securely every night, as will mobile telephones.

Pupils are given a talk about ICT and this covers the use of Facebook and other social network sites.

The PSHE programme is also used to help support the work of internet awareness and cyber-bullying.

The College aims to provide an information evening for parents during the year to discuss the issues of social network sites and access.

### **Sanctions**

Pupils caught trying to access any social network sites, through whatever means, outside of the controlled access times will be punished as detailed below:

- 1<sup>st</sup> offence    HSM caution and Sunday detention
- 2<sup>nd</sup> offence    Letter home plus Sunday detention
- 3<sup>rd</sup> offence    Deputy Head caution

### **Gaming and DVDs**

The main issues relating to gaming and the watching of DVDs focus around the following:

- The negative impact on work and study ethic
- Access to only age appropriate games and films
- Their addictive nature
- The illegal copying of games

- The difficulties of network access/traffic speed when such media are used
- The anger and frustration games can evoke in some pupils

The College has therefore concluded that the time pupils are allowed to play on games and to watch films will be limited from 4.00pm on Saturday to 6.00pm on Sunday. Games and DVDs may be allowed at prep break at the HSMs discretion.

Pupils must only watch and play games that are age appropriate. Any material that is not age appropriate will be confiscated and this will be returned to parents at the next opportunity.

### **Sanctions**

Pupils caught playing games or watching DVDs outside of the controlled times will be punished as detailed below:

- 1<sup>st</sup> offence      HSM caution
- 2<sup>nd</sup> offence     HSM caution and Sunday detention
- 3<sup>rd</sup> offence     Letter home plus Sunday detention
- 4<sup>th</sup> offence     Deputy Head caution
- 

However, the 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.

### **Cyberbullying**

The College's preventative measures and procedures for dealing with Cyberbullying are found in the Anti-Bullying Policy published on the College website

### **Mobile Phones**

Mobile phones may not be used during the school day. Members of staff confiscate mobile phones (passing them immediately to the relevant housemaster or housemistress who keeps them for 24 hours (first offence), 48 hours (second offence) or longer term confiscation with the involvement of parents (third offence).

The College does not normally expect staff and pupils to communicate with each other by text or mobile phones. The Educational Visits Policy explains the circumstances when this may be permitted: pupils' mobile numbers are deleted at the end of the visit.

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

### **Cameras**

The use of cameras, including those on mobile phones, is not permitted in lessons, Chapel, plays or concerts in any other College activity where they could justifiably be regarded as an interference or intrusion. While they may be used at matches or in the houses, they must not be used in changing or washing areas. Care must also be taken in pupils' bedrooms or dormitories that they should not be used in a way that could justifiably be regarded as intrusive or embarrassing. Staff may take and use images of pupils purely for work purposes and where possible such images will not be stored on personal electronic devices.

## **Safe use of personal electronic equipment**

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.

### **More information**

Pupils are encouraged to make use of the excellent online resources that are available from sites such as:

- Childnet International ([www.childnet-int.org](http://www.childnet-int.org))
- Digizen ([www.digizen.org.uk](http://www.digizen.org.uk))
- Cyber Mentors ([www.cybermentors.org.uk](http://www.cybermentors.org.uk))
- E-Victims ([www.e-victims.org](http://www.e-victims.org))
- Bullying UK ([www.bullying.co.uk](http://www.bullying.co.uk))

### **References**

[www.cyberbullying.org.uk](http://www.cyberbullying.org.uk)

Becta 'Acceptable Use Policy in Context: Establishing Safe and Responsible Online Behaviour

DCSF The Byron Review Action Plan (2008) [www.dcsf.gov.uk](http://www.dcsf.gov.uk)

Keeping our Schools Safe: Sir Roger Singleton (2009) [www.teachernet.gov.uk](http://www.teachernet.gov.uk)

Cyberbullying: A Boarding Briefing Paper: Veale Wasbrough, BSA

ISBA policy guidance

**September 2010**

**Review date: September 2011**