Cheltenham Bournside School
and Sixth Form Centre
11-18 Academy

E-safety & Information Technology Acceptable Use Policy

Approved Oct 2017

All school policies are reviewed by Governors annually

1 SCOPE OF THE POLICY

This policy applies to staff, students, volunteers, 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:

1. 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 Child Protection Officers.
2. 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.
3. The Senior Leader with oversight of continuous professional improvement (CPI) is responsible for ensuring that staff receive suitable training with regards to the content of this policy.

Child protection officers:

1. Take day to day responsibility for e-safety issues.
2. Have awareness of inappropriate on-line contact and the potential for grooming, cyber-bullying and radicalisation.

Head of IT Services & IT supporting staff:

The Head of IT Services and IT Supporting staff are responsible for ensuring that:

1. The school's technical infrastructure is secure and is not open to misuse or malicious attack.
2. Users may only access the network resources through a properly enforced password protection procedure.

3. Internet filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
4. They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
5. Their permissions and privileges to IT systems as domain administrators are used in accordance with this policy.
6. New staff confirm they have read this policy by email or online data collection.

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

1. They have an up to date awareness of e-safety matters and of the school e-safety & acceptable use policy and practices.
2. They report any suspected misuse of IT to the Head of IT Services or Child Protection Officer as appropriate.
3. All digital communications with students, parents/carers should be on a professional level and only carried out using official school systems.
4. Key messages of e-safety outlined in this policy are communicated to students if there is an expectation that they will use the school's learning platform (Frog), social networking or digital photographs/video in their work.
5. Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations as appropriate to their subject and study.
6. They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
7. In lessons where internet use is pre-planned and students are guided to sites, these should be checked as suitable for their use.
8. They report inappropriate websites that bypass filtering to IT Services.
9. They keep devices and computers secured such that students, parents and guests cannot gain access to personal data. This includes not allowing students to use their laptops logged in as a member of staff and ensuring that computers are logged out or locked when not being used.
10. Photographs are not published for students listed as 'no photograph'.
11. Published photographs do not identify the full name of the student.
12. Their use of social media is appropriate as outlined in the policy statements.
13. Personal data from the management information systems must not be stored on unencrypted drives or portable media.

Students:

13. Are responsible for using technology in accordance with the acceptable use guidelines published to parents via the learning platform and outlined below.
14. Are not permitted to use virtual private networks (VPN) or associated VPN apps to bypass school filtering.

Parents:

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

1. Digital and video images taken at school events.
2. Access to student records through ParentFrog and School Gateway.
3. Their children's personal devices in the school.
4. Virtual private networks (VPN), which can be used at home, but not in school as they create security vulnerabilities to our network.

3 POLICY STATEMENTS

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach as recommended by Ofsted. The education of students in e-safety is therefore 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.

1. The school has a planned e-safety curriculum including:
    - A 10 week project in Year 7 focussed on cyber-bullying.
    - Year 8 PSHE lessons on e-safety.
    - A 10 week project in Year 9 focussed on protecting their digital identity and footprint.
    - Year 10 PSHE lessons on e-safety.
2. Key e-safety messages are reinforced in assemblies to all year groups.
3. 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.
4. 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.
5. In lessons where internet use is pre-planned and students are guided to sites, these should be checked as suitable for their use.
6. 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.
7. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff

can request that IT Services can temporarily remove those sites from the filtered list for the period of study.

8. All users should keep their password for accessing school IT systems secure and should not share these. If users suspect their password has been compromised they should change it immediately.

Technical infrastructure/equipment, filtering and monitoring

1. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements for e-safety.
2. There will be regular reviews of the safety and security of school technical systems.
3. Servers, wireless systems and cabling will be securely located and physical access restricted as appropriate.
4. All users will have clearly defined access rights to school technical systems and devices.
5. All users will be provided with a username and secure password by IT Services who will maintain records of users and their usernames. Users are responsible for the security of their username and password.
6. The domain administrator passwords for the school IT system, used by the Head of IT Services and IT Supporting staff must also be available to the Headteacher or other nominated senior leader with responsibility for IT and kept in a school safe.
7. Data is kept securely on three physically separate locations in school to minimize data loss in the event of a disaster response.
8. The Head of IT Services is responsible for ensuring that software licences are valid and up to date for the required number of software installations.
9. Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list, or similar by the school internet service provider.
10. Students are kept safe from accessing terrorist and extremist material when accessing the internet in school through filtering in response to the 'Prevent Duty'.
11. Staff have access to unfiltered internet via a staff proxy but web addresses visited are recorded and may be monitored.
12. Users are required to report any actual or potential technical incident/security breach to the Head of IT Services.
13. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date anti-virus/malware software.
14. IT Services will provide temporary restricted access to school systems for guests, trainee teachers, supply teachers and visitors as appropriate.

15. Users are permitted to use school devices for personal use, but all use must be in accordance with this policy.

16. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring your own device (BYOD)

BYOD refers to users bringing their own technologies to use in the school.

1. BYOD should not introduce vulnerabilities into existing secure environments.
2. Connection to the internet is provided by a secure guest WiFi hotspot, and restricted WiFi hotspot for students. All WiFi hotspots are covered by the school's normal filtering systems.
3. Guest WIFI should only be used for educational purposes.

Use of digital and video images

1. When using digital images, staff should inform and educate students 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.
2. 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 should not be published or made publicly available on social networking sites.
3. Staff and volunteers 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 kept by the Business Centre.
4. The distribution of digital/video images to students and parents should only be done via the Learning platform or social networking by giving them to IT Services for uploading.
5. 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.
6. Students must not take, use, share, publish or distribute images of others without their permission.
7. Photographs published on the website, Learning platform or elsewhere 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, only the forename.
8. Students' full names will only be used on blogs and social networking when there is no accompanying photograph, including group photographs.
9. Parents may add their child to the 'no photograph' list by indicating this on the student data collection form sent to parents.

Data Protection

The school has a Data Protection Policy which should be read in conjunction with this policy.

Use of Social Media and Email

1. 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 school opening hours.
2. Users should be aware that whilst email communications are not routinely monitored this may be done at the discretion of the Headteacher.
3. Users must immediately report, to a teacher, line manager of 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.
4. Any digital communication between staff and students or parents/carers must be professional in tone and content.
5. All recorded comments about students, parents or staff on school data management systems must be professional in tone and content, such that it could be shared with the relevant stakeholder if requested. This includes SIMS and PAM, but is not exclusive to these systems.
6. Staff must not 'befriend' students or parents on social networking and maintain a 'professional distance'. Where there may be an exception to this granted for students or parents that are family members or close friends, this should be brought to the attention of the Headteacher.
7. No reference should be made in social media to students, parents/carers or school staff other than for reporting school news via the official school website and social networking accounts.
8. Such social networking accounts should only be created in consultation with IT Services.
9. Users should not engage in online discussion on personal matters relating to members of the school community.
10. Personal opinions should not be attributed to the school.
11. Users should ensure that security settings on personal social networking profiles are set to minimise the risk of loss of personal information.
12. Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
    a. Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
    b. Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
    c. Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.

d. Pornography.

e. Promotion of any kind of discrimination.

f. Threatening behaviour, including promotion of physical violence or mental harm.

g. Terrorism or extremism.

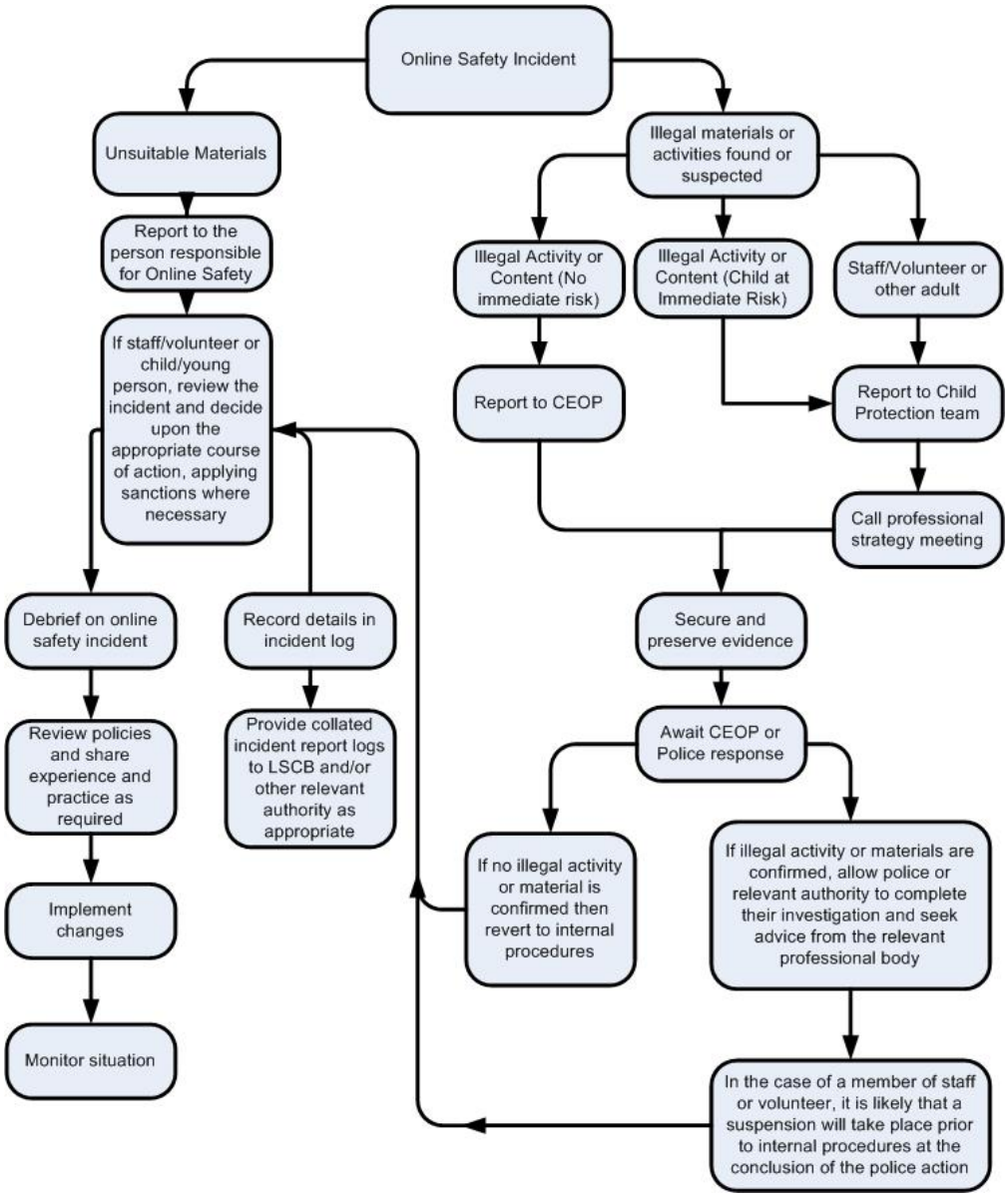
h. Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

13. Users should not use school systems to run a private business.
14. Users should not use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
15. Users should adhere to copyright guidelines.
16. Users should not reveal or publicise confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)
17. Users should not create or knowingly propagate computer viruses or other harmful files.
18. Users should not use school systems for gambling.
19. Users should not engage in Illegal file sharing.

4 RESPONDING TO INCIDENTS OF MISUSE

If there is any suspicion that the activty concerned may contain child abuse images, or if there is any other suspected illegal activity, the matter will be reported to the police.

The procedures outlined below will apply. The person responsible for Online Safety in this context is the Headteacher.



5 TRAINING

Training in e-safety policy will be offered as follows:

1. Through the annual CPI programme.
2. All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use agreements.

Acceptable use guidelines for students in their use of information technology at Cheltenham Bournside School

Cheltenham Bournside School is a "Technology enhanced learning school". We welcome students to bring tablet devices to school to use in their lessons, as directed by their teachers. We recognise that digital technologies including a range of devices and the internet have become integral to the lives of young people, both within and outside the school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, stimulate and promote effective learning. These acceptable use guidelines are intended to ensure:

1. That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
2. That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

For my own personal safety:

1. I understand that the school will monitor my use of the systems, devices and digital communications.
2. I will keep my username, password or passcode safe and secure – I will not share it, nor will I try to use any other person's username, password or passcode. I understand that I should not write down or store a password/passcode where it is possible that someone may steal it.
3. I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
4. If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
5. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

To ensure fair usage:

1. I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
2. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
3. I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

Respecting others:

1. I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
2. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
3. I will not engage in cyber-bullying, including sending inappropriate text messages or posts on social media that are likely to offend or upset others.
4. I will not take or distribute images of anyone without their permission.

Maintaining the security and integrity of IT systems:

1. I will only use my own personal devices in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
2. I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials. This includes material of a terrorist or extremist nature.
3. I will immediately report any damage or faults involving equipment or software, however this may have happened.
4. I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
5. I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
6. I will only use social media sites with permission.
7. I will not use virtual private network or proxy servers to bypass school filtering systems, or allow others, including my parents to access my device on the school network.
8. I will only use my own login credentials to access school systems. If I become aware of another user's password/passcode I will inform a teacher.

Copyright and trustworthiness of information:

1. Where work is protected by copyright, I will not try to download copies.
2. When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.