Bosworth Independent College

Computer Acceptable Use Policy Teachers and Other Employees

Reviewed	3rd January 2020
Next Review Date	July 2020
Lead for Review	Kevin Jones

Introduction

The following policy (referred to as 'AUP') outlines the ways that the computer and other technology can and should be used by all employees of the college. It also includes College's Firefly VLE and College-sponsored social networking sites.

All Bosworth's Computer policies are designed to ensure compliance with relevant parts of the General Data Protection Regulations – GDPR - (act of parliament 2018 and subsequent changes). This AUP should be applied by College staff and by College students (supported by College staff) in accordance with the GDPR.

Employees should be aware of the Acceptable Use Policy for students and that the details set out in that apply to staff. Consequently, the Student Policy is included below for the information of Staff.

The following are extra guidelines, which are specific to employees of the college:

1. Do not give personal addresses, telephone / contact details of any adult working at the school or any students at the school without their permission.

2. Whilst we are happy for staff to use the internet for their own use during their free time in a school day, staff should be aware that the computers are provided primarily for use directly related to the education of the students and the management of the college and this should take precedence over any personal use.

3. Use of names of students, or photographs of students, will require written permission from parents. This also applies to any work done by students, relating to their education at Bosworth College. Parental permission is given as part of our terms and conditions. When and if a parent or a student declines this, a record is kept and made available to staff on Engage.

4. Photographs of students should only be taken on College equipment. If a member of staff needs to take photographs of students for teaching or marketing purposes on their own equipment (e.g. phone or iPad), photos must be downloaded at the earliest opportunity to College equipment. They must then be deleted from personal equipment. Photos must also be deleted from email accounts that may be used or recycle bins.

5. College data cannot be stored on personal laptops or equipment UNLESS access to the appliance is password protected or the files concerned are encrypted. Passwords must not be available to users who are not College staff.

6. Do not download, use or upload any material and use material which is copyright.

7. Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material of a violent, dangerous or inappropriate sexual content.

8. Always respect the privacy of files of other users. Do not enter the file areas of other staff without their permission.

9. Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything which could be interpreted as libel. Be aware that email may not be secure and do not write anything that could be misconstrued or bring the College into disrepute.

10. Ensure privacy and confidentiality is maintained if accessing email remotely.

11. Arrange for suitable monitoring of students in your class, or those students who you have given permission to use the Internet facilities.

12. Ensure that all students have followed the correct procedures:
i. before starting the session,
ii. during each session, and
iii. on completion of the session.

13. Report any incident which breaches the Acceptable Use Policy immediately to the Vice Principal, Kevin Jones.

14. Staff must not use their personal Facebook accounts and other social networking sites to contact, be contacted by or in any other way inform students currently at the College. Extreme care must be taken if ex-students are contacted using these sites. The College accepts no responsibility and offers no protection for misuse, either deliberately or accidently, where ex-students of the College are involved.

15. In connection with use of computer systems, Staff must be aware of the place of the parents and families of Bosworth students. Staff use of social media must not compromise the interests of students, Staff, families or the public image of the College. Employees should report any use of information technology by parents or families that causes them concern. Staff should inform the DSL and Online Safety Officer (Karen Inman) or her deputies (Steve O'Hare, Kevin Jones or Craig Wilson) as soon as possible and never within less than 24 hours of any request for help or concern raised by parents and families.

16. Staff must remember that the internet can raise serious safeguarding issues with respect to students. Please remember to report to the DSL (Karen Inman) or her deputies (Steve O'Hare, Kevin Jones or Craig Wilson) as soon as possible and never within less than 24 hours anything that concerns you. This includes student

contact or access to cyberbullying (as perpetrator or victim), pornographic material, radicalising or extreme material, any other sort of inappropriate material, contact that may be sexual 'grooming' or the sharing of pictures, e.g. by sexting.

17. As is normal practice in schools, colleges and other workplaces, all network access, web browsing and mails on the school system are logged and routinely monitored to ensure the acceptable use policy has not been broken. For staff, this is normally performed only in the case of a concern that may represent a breach of the Policy. Such monitoring would occur only at the instruction of the Principal and would be managed by her or the Vice Principal. The College's obligations under data protection law, GPDR, safeguarding and employment law would be maintained.

18. Please ensure your area of the P:/drive is kept up-to-date and all out of date material is deleted.

Computer Acceptable Use Policy Students

Introduction

The use of the latest technology is actively encouraged at Bosworth Independent College but with this comes a responsibility to protect both students and the College from abuse of the system.

All students, therefore, must adhere to the policy set out below. It is the 'Acceptable Use Policy', called the 'AUP'. This policy covers all computers, laptops, smartphones and other electronic devices within the College, irrespective of who is the owner or whether used on or off College premises. Students sign a form on entry to the College and at the start of every academic year. A student's signature commits them to following this policy at all times.

Use of IT in the UK is governed by law and by the General Data Protection Regulation (GDPR). The GDPR is law in the UK under the General Data Protection Regulation Act 2018. So, following this Student Acceptable Use Policy and Student IT User Agreement is required in order to obey the law.

All students are expected to behave responsibly on the College computer network, as they would in classrooms and in other areas of the College.

In case of problems with IT and where, in this policy, it states 'contact IT', students should contact the College's IT Support email address on support@bosworthcollege.com Mr Mark May and Mr Chris Wood are available to support students. If students are concerned about safeguarding or Behaviour Policy issues, they should contact a member of staff. This can be your Personal Tutor (PT), Course Director or House-Parent or one of the designated safeguarding leads (Ms Inman – the senior DSL; Mr O'Hare – the Head of Boarding; Dr Craig Wilson – the Principal; Mr Jones – the Vice Principal. Such issues might be cyberbullying, sexting, someone inappropriate contacting you or someone contacting you in an inappropriate way or anything mentioned below.

The Policy:

1. Personal Safety Online:

   1.1. Always be extremely cautious about revealing personal details and never reveal a home address, phone number or email address to strangers.
   1.2. Do not send anyone your credit card or bank details without checking with a teacher.
   1.3. Always inform your teacher or another member of staff if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.

1.4. Do not play with or remove any cables that are attached to a College computer.
1.5. Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
1.6. Do not arrange to meet with anyone you have met on the Internet – people are not always who they say they are.
1.7. If in doubt, ask a teacher or another member of staff.

2. System Security:

2.1 Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending email whilst masquerading as another person, or accessing another person's files. Attempting to log on as staff or as IT will be dealt with severely. You are only permitted to log on as yourself.
2.2 Do not give out your password to any other student – if you do and they do something wrong logged on as you, you will be held responsible. If you suspect someone else knows your password change it immediately
2.3 Do not make deliberate attempts to disrupt the computer system or destroy data; e.g. by knowingly spreading a computer virus.
2.4 Do not alter college hardware in anyway.
2.5 Memory sticks should be used on workstations that have USB ports at the front; do not unplug cables to insert the memory sticks at the front or back. You must give the workstation a few seconds for it to find the drive before unplugging the memory stick. If in doubt, see the IT person.
2.6 Do not knowingly damage or misuse headphones or any other external devices e.g. printers, mice.
2.7 You may use your own headphones only if there is a headphone socket on the front of the computer. Do not attempt to plug them into the back.
2.8 Do not attempt to connect to another student's laptop or device while at College. Establishment of your own computer network is not allowed.
2.9 Do not eat or drink whilst using the computer.

3. Inappropriate Behaviour:

3.1 Do not use indecent, obscene, offensive or threatening language.
3.2 Do not post or send information that could cause damage or disruption.
3.3 Do not engage in personal, prejudicial or discriminatory attacks.
3.4 Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
3.5 Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.
3.6 Do not post or send private information (including images) about another person without them agreeing first.
3.7 Do not use the Internet for gambling.
3.8 Bullying of another person either by email, online or via texts will be treated with the highest severity.

3.9 Do not access material that is profane or obscene, or that encourages illegal acts, violence, or discrimination towards other people.
3.10 If you mistakenly access such material, please inform your teacher or another member of staff immediately or you will be held responsible.
3.11 If you are planning any activity which might risk breaking the acceptable use policy (e.g. research into terrorism for a legitimate project), an appropriate member of staff of the relevant subject must be informed beforehand.
3.12 Do not attempt to use proxy sites on the Internet.
3.13 Do not take a photo of another student or member of staff without their permission.
3.14 Never text or send pictures of yourself or other people which are or could be thought to be sexual or pornographic. 'Sexting' is a crime dealt with by the police

Inappropriate Behaviour relates to any electronic communication whether email, blogging (e.g. online diaries), texting, journal entries, writing on social media (Facebook, Snapchat, Instagram etc.) or any other type of posting / uploading to the Internet.

4. Email:

4.1 You should check your College email at least once a day for new messages.
4.2 Do not reply to spam mails as this will result in more spam. Delete them and inform IT.
4.3 Do not open an attachment from an unknown source. Inform IT as it might contain a virus.
4.4 All emails sent outside the College reflect on Bosworth Independent College so please maintain the highest standards.
4.5 Do not use email (including webmail) during lessons unless your teacher has given permission.
4.6 Do not send by mail any files above 5mb. Please ask IT if you require this temporarily.
4.7 Do not send or forward annoying or unnecessary messages to a large number of people e.g. spam or chain mail.
4.8 Do not join mailing lists without the prior permission of IT.
4.9 Only send mail to a distribution list if you really have to.
4.10 If you receive an email sent to you in error, please inform the sender immediately.

5. Plagiarism and Copyright:

5.1 Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else.
5.2 You should respect copyright. Breaking copyright law occurs when you

reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner. This includes music files and the copying of CDs etc.

6. Privacy:

6.1 All files and emails on the system are the property of the College. As such, system administrators and staff have the right to access them if required.
6.2 Do not assume any email sent on the Internet is secure.
6.3 All network access, web browsing and mails on the College system are logged and routinely monitored to ensure the acceptable use policy has not been broken. At any point IT can see what is happening on any computer screen without your knowledge.
6.4 If you are suspected of breaking this policy, your own personal laptop / device and mobile phone can be searched. Refusal to allow this is likely to lead to you being asked to leave the college.
6.5 The College reserves the right to randomly search the Internet for inappropriate material posted by you and to act upon it.

7. Software:

7.1 Do not install any software on the College system.
7.2 Do not attempt to download programs from the Internet onto College computers.
7.3 Do not knowingly install spyware or any sort of hacking software or device.

8. Laptops and PDA's

8.1 If you wish to use your own personal laptop in a Boarding house, you can connect to the Wi-Fi network, which will require you to use your college username and password. If you have problems connecting, then you can contact Bosworth Independent College staff during college time.
8.2 The network will close at 11.30pm on Sunday to Thursday and 12.30am Friday/Saturday nights.
8.3 The bandwidth is restricted where Skype users will have the highest priority and YouTube users will have the lowest priority. Any students using torrent software for downloading movies/music/etc (i.e. Utorrent etc.) will be blocked. These users will be removed for the network by the IT manager because they will slow down the network significantly causing speed and access issues to all other users in the Boarding House. The user will be asked to remove this software before they can access the network again.
8.4 Your laptop or device must have adequate security protection, such as, up-to-date anti-virus software installed. Your laptops or device will be

scanned automatically to ensure this is so. Do not attempt to use hacking tools.

8.5 Senior Houses allow students to have uncontrolled access to the Internet and, while it is recognised that policing the use of IT will be difficult, students must:

8.5.1 Obtain written permission from parents/guardians to be allowed to move to a house with its associated freedoms

8.5.2 Agree that "they will not download obscene/pornographic/racist etc. material from the Internet" as stated on the parental agreement

8.5.3 Understand that poor punctuality will result in a move back to a supervised Boarding House (e.g. where it is clear students are using laptops excessively late at night)

8.5.4 Have been briefed by their Personal Tutor on the full details and rationale of the college CAU policy

8.6 The use of webcams is only allowed in contact using Skype (or similar) to contact family and friends, but we strongly advise not to use the HD facility Skype offers.

9. Mobile Phones:

9.1 Do not use a mobile phone during lessons except in an emergency.

9.2 Do not take photos or videos with a phone during lessons unless the member of staff has given permission.

9.3 Do not take photos of people without their permission.

9.4 Bullying by text or any other method will be treated in the same severe manner as any other form of bullying.

9.5 Do not attempt to hack into someone else's device via Bluetooth or any other method.

9.6 Teachers and Supervisors have the right to confiscate mobile phones if they are used inappropriately. This may be until the end of the College day for a first or second offence, but longer if you persist in breaking this guideline.

10. Music / Video players e.g. iPods and phones:

10.1 The use of such devices is banned during lessons unless the teacher has given permission.

10.2 Do not connect such a device to the College network / College computers.

10.3 Do not break copyright laws by illegally swapping music / video files.

10.4 Headphones should not be worn in class, corridors, in the canteen, or when moving between the College buildings.

10.5 Do not listen to music in lessons whether via CDs or MP3 etc or streaming. unless the teacher has given permission.

10.6 You can listen to music via MP3 players etc. during Study Hall sessions but it must not disturb other students.

11. Other Electronic Devices:

The IT policy above also covers other electronic devices such as laptops, tablets and mobile phones while they are being used at College. However, none of these devices are covered by the College's insurance and the College accepts no liability for them. All devices should be security marked and kept locked away where possible. This also includes items such as digital cameras and personal DVD players etc.

12. General and Best Practice

12.1 Think before you print. Printing is expensive and consumes resources, which is bad for the environment. Only College work should be printed off and care should be taken not to print entire documents when only a few pages are needed. Boarding House Supervisors can print work for you.
12.2 Priority must be given to students wishing to use the computers for College use.
12.3 Always log off your computer when you have finished using it. Do not lock the computer so that others cannot use it.
12.4 Always back up your work if you are not saving it on the College system. Work saved on the College system is backed up every night for you but be careful if you only have a copy of your work on a memory stick as you could lose it.
12.5 Avoid saving or printing huge files (e.g. above 5mb). If in doubt, ask IT.
12.6 If someone makes you an offer on the web or via mail, which seems too good to be true, it probably is.
12.7 Passwords should be alpha numeric i.e. contain both letters and numbers.
12.8 Observe health and safety guidelines; look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted.
12.9 Be considerate and polite to other users.
12.10 Housekeep your email regularly by deleting old mail.
12.11 Leave your computer and the surrounding area clean and tidy.
12.12 If a web page is blocked that you feel you have a legitimate use for, please ask IT and it can instantly be unblocked if approval is given.
12.13 The Internet can become addictive. If you feel you are spending too long on it please ask a teacher or another member of staff for advice about whether this is safe.
12.14 If you are leaving the college for good please ensure you have saved any files or email you want to keep to a memory stick or CD to take home, as these files will be deleted.
12.15 If in doubt, ask a member of the IT department.

13. Sanctions:

13.1 Sanctions can vary depending on the severity of the offence, from a warning or withdrawal of Internet use, to suspension or expulsion. Any breach of any law or act may lead to the involvement of the police or any other relevant authority.

Computer Acceptable Use Policy - Students (summary)

This agreement includes all computers, laptops, smartphones and other electronic equipment in College.

If you have any problems, contact IT support at support@bosworthcollege.com

Do	Don't
• tell your teacher if you visit a website, or receive a message, which makes you feel uncomfortable. • be yourself on the internet, never pretend to be someone else or use proxy sites. • ask permission before you take a photo of any other student or a teacher. • keep your password to yourself – if you think someone else knows it, change it! • ask another person's permission before you send anyone a photo or information about them. • tell a teacher at once if you see any material which encourages radicalisation or illegal acts. • respect copyright (it is a crime to use copyright material). • get proper security protection on your own laptop, smartphone etc. • make sure you turn off your webcam after using Skype and cover it with a cloth/tissue • make sure your music (if you use it) does not disturb other students in Study Hall. • log off properly when you finish. Don't lock the computer! • use a password with letters and numbers in it. • ONLY use the sockets/USB ports on the FRONT of the computer.	• give ANYONE you do not know personal information (home address, bank details, phone number, email…). • send or ask anyone to send sexual or erotic pictures. 'Sexting' is illegal and is reported to the police. • move or change any cables or hardware (printers, headphones…) on a College computer. • arrange to meet up with anyone who contacted you on the Internet. • access anyone else's files. • eat or drink while on the computer • alter the hardware or College software in any way, or harm it (e.g. by introducing a virus). • reply to spam emails, do 'chain mail', or open attachments from any unknown sender. • access or create obscene, offensive or illegal material. • take the ideas or writing of someone else and present it as your own ('plagiarism'). • install any software, or download programs or spyware, on College computers. • break the law by illegally swapping music/clips. • connect your device to a College computer. • Use a computer for bullying or gambling

- All files and emails on the College system are the property of Bosworth College. College staff have the right to look at them if they need to. College reserves the right to search your laptop, smartphone etc if necessary.
- The network will close at 11.30pm (Sunday to Thursday) and at 12.30am on Fridays and Saturdays.
- Senior House students are required to sign a separate agreement.
- Your laptop, smartphone etc. is not covered by the College's insurance and the College cannot accept liability for them. They should be security marked and kept (locked away) in a safe place. Students must place phones in the blue/red boxes

provided during lessons and Study Halls. Phones/translators etc can only be used in lessons if the teacher says it is OK.

- Cyberbullying is very serious and will be treated the same as any other kind of bullying.
- Print responsibly: only what is necessary.
- Always back up your work if you are not saving it on the College system (College backs up everything on the system every night).
- If you do need to use a webpage that is blocked, ask IT who can unblock it if your teacher/Course Director approves it.
- Sanctions can vary depending on the severity of the offence, from a warning or withdrawal of Internet use, to suspension or expulsion. Any breach of any law or act may lead to the involvement of the police or any other relevant authority.