Bentley Wood
High School for Girls

IT POLICY

GB Committee Responsible:	**Finance and Site**
Reviewed by:	Raj Patel
Review Date:	May 2018
Ratified by Committee:	13th June 2018
Next Review Date:	19th June 2019

Bentley Wood High School
IT Policy

Introduction

Technology is rapidly changing everyone's lives. Students and learning habits are evolving. Schools are the hub of this evolution, an organisation which can take advantage of the possibilities technology can bring to our mind, creativity, inspiration and opportunity for all.

Ensuring students appreciate, utilise and capitalise on their IT educational experience throughout their lives is a challenge and a responsibility of our school.

The development of technology is changing at home and in the community. Its impact on the lives of individuals continues to grow and it is essential that our students can take advantage of its opportunities and understand its effects. Therefore, it is important that students in our school gain the appropriate skills, knowledge and understanding to have the confidence and capability to use IT throughout their lives.

Vision of IT in our School

"Bentley Wood High School aims to prepare IT/ learning infrastructures fit for the 21st Century learner. We intend to engage our community, expand our curriculum and extend our IT provision in novel and imaginative ways to benefit all those to seek to learn"

We aim:

- To equip student with the skills necessary to learn outside the classroom over time to become lifelong learners.
- Be fully aware of the risks and intelligence IT skills can bring to learning and their everyday lives.
- To encourage students to become, develop a growth mindset philosophy, self-regulating their learning and empower them using IT as the key tool.
- To provide appropriate opportunities for all students to acquire Computing skills throughout the curriculum;
- To explore learner's attitudes towards IT, its value for themselves, others and society;
- To provide opportunities for students to work collaboratively locally and globally;
- To promote the use of IT for inclusion purposes;
- To implement an online study environment giving access to high quality resources and learning materials online, accessible anytime anywhere where learners can collaborate effectively.
- To effectively meet students' needs through the use of IT;
- To provide staff development in order to improve teachers' IT skills;
- To promote e-safety and provide educational support on wider IT issues;
- To keep abreast of emerging technologies and evaluate the benefits for educational purposes.

Monitoring, Evaluation and Review

The school will endeavour to regularly audit the provision of IT resources, the quality of students' learning experiences and staff development needs through embedded audit procedures linked to the school development planning process.

The School's Curriculum Organisation

Computing lessons are taught discreetly in Key Stage 3 with 1 period a week in Year 7 and 2 periods 2 periods over a week in Year 8. Students can choose to continue to study Computing in Year 9 as one of their option choices. Schemes of Learning include guidance on how to conduct activities online safety; this will be delivered to all year groups at least once a year. Cross-circular use of IT will be mapped and departments will be encouraged to develop innovate ways to promote learning through IT. A continuous support programme for staff including suitable training and specialist help will be implemented.

Equal Opportunities

All students regardless of race, gender or ability should have the opportunity to develop IT capability.

We ensure that all our students:

- have equal access to IT resources (including outside school);
- have equal opportunities to develop IT capability;
- use software which is appropriate to their ability.

Students with Special Educational Needs

Students with Special Educational Needs benefit from using Information Technology as it enhances access to the curriculum, and this in turn encourages motivation and the development of skills ensuring significantly higher achievements. Therefore, the opportunities to utilise IT should be maximised, supported and monitored.

School Network

Students are expected to use IT only for their schoolwork. If they need to use it for any other purpose, they should first seek permission from a member of the IT staff.

Students are provided with their own account on the school network and are expected to keep secret the password to this account. If at any time, a student believes that their password has become known to others, then it is the student's responsibility to ask for the password to be changed as soon as possible .Students must only log onto their account on the network and are not allowed under any circumstances to log on as anyone else.

Students are allowed to use only the software that is installed on the school computers.

Sixth form students who have their own devices including smart phones and who wish to bring

these into school will be given permission to access the school network if the device conforms to school security checks:

- The security of the school information systems will be reviewed regularly;
- All suspected or actual breaches of IT security shall be reported to the Headteacher who should ensure a speedy and effective response to be made to an IT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements.
- Virus protection will be updated regularly;
- Personal data sent over the Internet will be encrypted or otherwise secured and will follow GDPR regulations
- The use of portable media must conform to virus protocols and any student data copied to this media must be encrypted. The network team will aid this process;
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail;
- Files held on the school's network will be regularly checked so it conforms to acceptable use;
- Securus software is installed to audit both user network and Internet activity;
- The School use the pan-London LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The School will have in place a disaster recovery plan and will test the plan yearly;
- Network Manager will review system capacity regularly;
- The School recommends staff and students use its licensed Microsoft Cloud Storage services i.e. One drive to store internet based files.
- All software installed on the school network will adhere to the licensing regulations of that software and used in strIT accordance with the license agreement. Furthermore personal software should not be installed onto school hardware.

e - Safety

Computer networks, including those which may be accessed via the Internet, are an important aspect of information technology education. However, they present possible risks to the moral and social development of students, particularly in terms of the nature of some of the material which may be obtained via the Internet.

To prevent students having access to any materials on the internet which may be illegal, defamatory, inaccurate, obscene or offensive, the school's internet access will be through a recognised educational service provider, offering a filtered service.

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety

issues which may arise in classrooms on a daily basis.

All staff are made aware of individual responsibilities relating to the safeguarding of students within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

Students using the school's computing facilities will be expected to comply with the rules outlined in **Appendix 1**

Managing Internet Filtering

- If staff or students discover unsuitable sites, the URL must be reported to the Network team;
- Students using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child Exploitation & Online Protection Centre*).*

Authorisation of Internet Access

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications;
- All staff and students must read and sign the 'Acceptable Use Policy" before using any school IT resource;
- Students must apply for Internet access individually by agreeing to comply with the e- Safety Rules;
- Parents will be asked to sign and return a consent form for student access.

How will risks be assessed

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The school does not permit the use or activation of digital, electronic, or other recording technologies to be used on school premises except those devices that are for the clear and direct use by teachers, and a teacher's permission, to facilitate students learning.
- Due to the nature of Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material

accessed, or any consequences of Internet access.

Managing Email

As part of the school's on-going development of the IT programme, we provide a school e-mail account for all students. Students are expected to use school email for schoolwork only as and not for personal purposes. School email will be filtered and should not be regarded as private. We reserve the right to read email if we consider it necessary.

- Students may only use approved school e-mail accounts;
- Students must immediately tell a teacher if they receive offensive e-mail;
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;
- Access in school to external personal e-mail accounts for staff is acceptable but excessive social email use which can interfere with learning and may be restrITed.
- E-mail sent to external organisations should be written considerately and carefully with attention to net etiquette.

Managing Social Networking a n d Personal Publishing

- The school will block/filter access to Social Networking and Newsgroups sites unless deemed as educational and authorised by a member of the Leadership Group;
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas;
- Teachers' official blogs or wikis should be password protected and run from the school website.
- Teachers are not allowed to run social network spaces using personal email/accounts. They may use school network accounts which can be setup correctly to safeguard conversations between teaching staff and students. Teachers should seek advice and support from the IT Network team when implementing social media services for educational use.
- Teachers are to ensure correct privacy settings are implemented on personal social networking sites to protect their private and personal information.
- All staff, governors, and volunteers should note that the schools existing HR policy, sections 1.1.5 and 1.2.3 provide explicit guidelines on the expectations and professional conduct of staff when using social networking sites.
- The School should be aware that bullying can take place online and is committed in providing support and advice to all students.

Managing Emerging Technologies

Bentley Wood High School is committed to developing innovative teaching practices through the use of IT.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school;
- Technologies which reduce power consumption, reduce C02 emissions and support the schools drive to become more cost effective and efficient will be investigated and where appropriate implemented. E.g. online storage;
- The school will investigate and trial new technologies such as, open networks, collaborative learning and mobile technologies and will work within the Health and Safety guidelines.

Managing Complaints

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Complaints about staff misuse will be referred to the Headteacher.
- The school reserves the right to remove internet access for any user on the network or computer access for a period, which could ultimately prevent access to files held on the system.

Appendix 1 – Acceptable Use Policy - Staff Guidelines

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers;
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk;
- Activities such as trading online, for personal or financial gain using the school network or equipment is not acceptable e.g. trading shares.
- Using the schools IT equipment including tablets outside of school hours is permissible as long as this does not bring the teaching profession or school into disrepute is used for legitimate purposes.
- Always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses;
- Always check mobile equipment (e.g. laptops, tablet PCs, portable technology etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network;

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password;
- Always be wary about revealing your home address, telephone number, school name, or photographs to services on the Internet;
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- Familiarise and adhere to GDPR and data protection laws and school protocols.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk;
- Computer storage areas, files and communications are reviewed and monitored by the Network
- Management Team to ensure that you are using the system responsibly.

Internet

- Staff should access the Internet only for activities which do not affect their professional duties.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted;
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street;
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer;
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of IT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- Emails sent to an external organisation should be written carefully and considerately in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff should not attach unencrypted sensitive data to emails.

Please read this document carefully. Only once it has been signed and returned will access to the network will be permitted. Breaches in the above provisions could lead to an investigation and a disciplinary action. Additional responses may be taken by the school in line with existing policies such as the HR policy. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: _____ Signature: _____

Acceptable Use Policy - Student Guidelines

The school has provided computers for use by students, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers;
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the IT equipment;
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate;
- Always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses;
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software, and ensure they have been found to be clean of viruses, before connecting them to the network;
- Protect the computers from spillages by eating or drinking well away from the IT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password;
- Always get permission before revealing your home address, telephone number, school name, or picture to people you meet on the Internet;
- Other computer users should be respected and should not be harassed, harmed, offended or insulted;
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk;
- Computer storage areas (including cloud based files) will be treated like school lockers. Staff may review your files and communications to ensure that you are using the system responsibly.

Internet

- You should access the Internet only for study or for school authorised/supervised activities;
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted;
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws;
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms are not permitted;
- People you contact on the Internet are not always who they seem. Always ask a parent/guardian or teacher to go with you if you need to meet someone who you only know from the Internet or via email.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street;
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer;
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strITly forbidden.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Student Name: _____ Signature: _____

I have read and understand the above.

Parent/Guardian Name: _____ Signature: _____

Responsible Use of IPad - Staff guidelines.

- Users must use protective covers/cases for their iPad.
- The 4 digit pin code enabled at all times. This is not to be switched off.
- Applications bought by the school remain the property of the school so please do not transfer apps to your personal computers.
- Staff are advised to create their own ITunes account if they want to backup files to iCloud.
- It is a user's responsibility to keep their iPad safe and secure.
- Items deleted from the iPad cannot be recovered.
- Accessing Inappropriate Materials – All materials on the iPad must adhere to the IT Acceptable Use Policy. E.g. Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- The whereabouts of the iPad should be known at all times. The iPad have an app which monitors its location if misplaced or stolen. Please be aware of this fact as the network team can track its location outside school at any time.
- IT Technicians/Network Manager/Head Teacher must be notified immediately if an iPad is lost or stolen
- Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strITly prohibited.
- Bentley Wood School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.
- Lost or stolen iPad will not be replaced by the school. Please make sure your house insurance covers you for this device.
- The iPad is subject to routine monitoring by the School and should be surrendered if required.