Bentley Wood

High School for Girls

IT POLICY

GB Committee Responsible:	**Finance and Site**
Reviewed by:	Kieran Robinson and Paola Boyadjian
Review Date:	05 March 2024
Ratified by Committee:	12th March 2024
Next Review Date:	March 2025

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 keytool.
- 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 andsociety;
- To provide opportunities for students to work collaboratively locally andglobally;
- To promote the use of IT for inclusion purposes;
- To implement a Virtual School environment giving access to high quality resources and learning materials online, accessible anytime anywhere where teachers and learners can collaborate effectively.
- To effectively meet students' needs through the useof IT;
- To provide staff development in order to improve teachers' IT skills;
- To promote e-safety and provide educational support on wider ITissues;
- To keep abreast of emerging technologies and evaluate the benefits for educationalpurposes.

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. 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 safely; this will be delivered to all year groups at least once a year and also through the PSHE programme across all Key stages. 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 including safety online.

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 Encompassing Cloud Services

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. This is done on a weekly basis by the Senior Engineer. All requests for change are done with security in mind;
- All suspected or actual breaches of IT security shall be reported to the Headteacher who should ensure a speedyand 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.
- Advice will be sought from our DPO as soon as the school becomes aware of the breach.
- Virus protection will be updated regularly;
- Personal data sent over the Internet will be encrypted or otherwise secured and will follow UK GDPR regulations
- Portable media such as USB sticks or external hard drives should only be used to store personal data when authorised by the Operations Manager and must conform to virus protocols and any student data copied to this media must be encrypted. The network and data 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;

The school monitors IT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- Monitoring software is installed to audit both user network and Internet activity;
- The school uses a combination of Smoothwalland Sophos on premise web filter, and Securus monitoring software which allows real time, intrusive monitoring and filtering. This blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature

- Staff are made aware through training sessions and staff induction processes that Internet traffic is be monitored and traced to the individual user as per Keeping Children Safe in Edcucation Sept 2024. Discretion and professional conduct is essential.
- The School will have in place a disaster recovery plan and will test the plan yearly. Backups are tested on a weekly basis when the Senior Engineer is on site and is part of the Network Manager's daily checks. The system is brought down and up again twice a year;
- 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 strict accordance with the license agreement. Furthermore, personal software should not be installed onto school hardware.

Online 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.

Online 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 online 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 online safety and know what to do in the event of misuse of technology by any member of the school community.

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation. Only designated SLG and the DSL are permitted to investigate and view content on students devices.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data 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 protection policy.

Staff email:

- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Professional language must be used at all times in communication.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. All breaches are to be reported to the Operations Manager responsible for UK GDPR at the school. This is line with our UK GDPR policy and

expectations.

- If staff send an email in error which contains the personal information of another person, they must inform the Operations Manager immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

Virtual School

Microsoft 365 has enabled Bentley Wood High School to historically operate a virtual school when required. This virtual school can be launched again if the situation requires. The items below relate to the principle of a Bentley Wood virtual school using our Microsoft 365 platform.

Vision & Principles

- To maintain our great learning school community
- Working & staying together as a community & family
- Maintaining our high quality of education for our girls
- Ensuring the girls continue to personally develop
- Continue to teach the girls about staying safe
- Feeding back to the girls about their work and inspiring them to learn more
- Continue to celebrate effort and achievements
- Maintain our great relationships with the girls and each other
- Develop excellent virtual teaching and learning practice for now and in the future

Key Protocols

- All staff have had safeguarding training on how to keep themselves and students safe online.
- Students and staff know how to report concerns.
- SEND, EHCP and other vulnerable students are carefully monitored and communicated with to ensure their needs are met
- All students and staff use Microsoft Teams to teach and communicate with each other
- No other method of video communication platform is permitted e.g. Zoom, What’s App - besides Teams
- Teachers should use to use Arbor to text message and email parents
- Audio chat is enabled during online meetings with students. Video options are enabled by the teacher
- All video lessons that are recorded are to be uploaded only to Stream no other platform is permitted

- Live lessons with either audio or video options are enabled for certain groups.
- PSTN calls may be enabled for certain users via Teams e.g. Safeguarding leads, HOY to keep in contact with students and families. This maintains their privacy
- Teachers are not obligated to video call or live teach
- Attendance and engagement is carefully monitored. Follow up calls are made and escalated where necessary
- The call facility is disabled for all students
- Protocols and guidance relating live video meetings is including in the Appendix.

Expectations (Students)

- Bentley Wood Virtual School etiquette current classroom behaviour and expectations should be mirrored in our virtual school.
- Address teachers and other students politely and appropriately e.g. no use of slang-
- Ensure the content you are posting is suited to the Team's purpose- Respect peoples' privacy by not taking pictures or videos of teachers or other students-
- Be an active participant – you are expected to be available online when required and respond to your teachers/peers and actively contribute to discussions
- Complete all assigned classwork and homework tasks set via MS Teams.

Managing Social Networking and 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 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. Formal complaints will follow the school's complaints policy.

Appendix 1 – Acceptable Use Policy - Staff Guidelines

The school has provided computers and mobile devices 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 devices 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

- Using the school's 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.
- Any loaned device such as a tablet or iPad must remain in the possession of staff, should only be used by them and should be securely stored when not in use. All associated items, including the charging cable should be kept in good order.
- Ensure that any loss or damage should be reported to the IT Network Manager immediately.
- If staff leave the employment of the School, then these devices returned to IT Support prior to their official leaving.
- Personal photographs or video should not be stored on the device
- Where photos or videos have been taken of pupils using a school device for the purpose of teaching and learning these should not be retained for any longer than absolutely necessary.
- Any confidential pupil data stored on staff's devices must be deleted once it is no longer needed.
- Staff device are configured by the School Mobile Device Management System. Staff must not attempt to change these settings or remove it from the Management System. VPN (Virtual Private Network) apps must not be used.
- iPads are set up to require a six-digit passcode and to lock automatically after two minutes of inactivity. This setting must not be changed.
- Activate iCloud to ensure that data remains safe in the event of loss or damage to an iPad.
- Insurance cover provides protection from the standard risks whilst a loaned device is on the School site but excludes theft from a staff member's home, car or other establishments. Should a loaned device be left unattended and it is stolen, staff will be responsible for its replacement.
- Activities such as trading online, for personal or financial gain using the school network or equipment is not acceptable e.g. trading shares.
- USBs and other portable storage devices are not to be used to store sensitive information unless encrypted and approved by the Operations Manager. Staff should use our Office 365 cloud services to store and retrieve files.

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 UK 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;

- Cloud 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.

Virtual School

Our professional virtual school environment is Microsoft Teams. Groups should only be set up and managed by a member of staff for school business. No other platform is to be used.

The Key Protocols in this document including online safety are to be adhered to.

It is strongly recommended that staff use the call facility within Teams to make telephone calls if needed, when not on school premises. This can be set up for selected users should the school return to teaching via the virtual school.

When accessing the network including our Cloud services School staff must not:

Transfer any material that could be deemed offensive, harmful or illegal from outside the School to the School network. This includes transfer by Internet or by any form of removable media.

Share any confidential or whole school documentation, such as that on the Staff Shared drive, with anyone from outside the School.

Transfer or store any confidential information onto other Cloud services such as Dropbox or Google Drive. The only cloud storage that may be used is the School OneDrive account

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 or links 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 SLG. 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.

School Equipment

- Only use the allocated IT devices for educational purposes. Activities such as buying or selling goods are inappropriate and are not permitted.
- Do not install, attempt to install or store programs/software of any type on the computers without permission.
- Respect, and do not attempt to bypass security in place on the IT devices, or attempt to alter the settings.
- Do not write, or publish anything using any device or computer that you would not be prepared to show your parents, the head teacher or a future employer.
- Do not be obscene either in the words that you use or the content that you view. This includes material that is violent, racist or adult in nature.
- Respect the laws of copyright and ensure that sources used are referenced appropriately.

Security and Privacy

- Do not share content that puts you, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or your location and tell a member of staff or your parent/carer should someone ask you for any of these details.
- Protect your work by keeping your password to yourself; never use someone else’s logon name or password;
- 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

- When accessing the internet at school or on school equipment, it should only be 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;
- '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.

Virtual School

To support continued learning outside the physical classroom we use Microsoft Teams.

- Students are unable/may not attempt to call, chat or set up private groups between each other on Microsoft Teams (this feature has been disabled).
- You are unable/may not attempt to start or record a meeting/lesson (this feature has been disabled).
- You are not permitted to share recorded videos/lessons made by teachers within or outside of your Teams account
- Your background is set to blurred and cannot be changed if in a conference meeting which involves a camera. The teacher controls this feature.
- You should think carefully about what is acceptable language and follow our BWHS Virtual School Expectations as outlined in this policy.

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 or click on links 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 strictly 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:____________________________

Appendix 2

Bentley Wood Virtual School – Live Video Meeting Guidance and Protocols

Please use this guide in conjunction with the current IT policy which outlines our Virtual School rationale.

Staff Protocols

Your teachers should follow these guidelines when setting up a live video meeting with students:

- Staff should try to give reasonable prior notice to students if they intend to schedule a live meeting with video enabled. Best practice is to schedule this meeting in advance in the calendar tab.
- Make sure that the room you are going live in is clear of things that might embarrass you. Specifically, look at your walls and try to pick one that has a plain background that people will not take offence at or find humour in.
- Where available use the 'change background affects' feature and set to blur or another appropriate image.
- Staff should ensure that any live meeting between students which is recorded is stored in Streams only and let participants know that it is being recorded.
- Everyone should ensure that a video meeting is taken in an appropriate location and that staff are appropriately dressed.
- Staff can disable student audio when managing student participation and when necessary.
- Staff must "End the meeting" after the event.
- Please note if you "stop incoming video" then students can still see each other.
- One to One video calls are not recommended for KS3/4 students unless authorised by a member of SLG for certain circumstances e.g. counselling.
- If you are sharing your screen make sure that you do have anything running in the background which you do not wish to share for example an online order with your home address.
- Please report and manage inappropriate online behaviour calmly.
- Any safeguarding concerns as always should be reported to the safeguarding team.

Advice for students and staff before a video meeting

- Check settings before you go live! Test this by selecting the 'Meet now' button under the video camera at the bottom of the chat page – this shows the live feed before the call. This way you can see what others see before you go 'live.
- Explain to your parents/carers you have a live meeting. Can they help you by keeping your surroundings quiet enough for you to engage with your learning? If your parents know and understand what it is you are trying to achieve, then they will help make sure that it all goes smoothly.
- Set your background to blur if your device allows this. Most laptops have this feature but many mobile phones do not. Select the three dots when starting a meeting to action this setting.
- Live video is not compulsory and optional but helps everyone to engage more interactively.
- Sit still and quietly and listen to the sounds around you. If you can hear noises, then there is a high chance that people in your meeting will too. Before starting, see if you can find a quieter place or attempt to control what is happening in your surrounding environment.
- Consider using headphones if you have a set so that you can hear clearly.

Advice during in a live video meeting:

- Be on time

- Start with your camera off and microphone muted and wait to be invited by the teacher.
- Have your video and audio turned off until invited to switch on by the teacher.
- Make sure you mute any audio on your device and then unmute when you need to talk to the teacher. This is because background noise and competing voices can be a problem in large groups.
- Understand that the rules used at school also apply in a virtual classroom.
- Use the “Chat” feature to ask questions of your teacher. This way your teacher can answer you directly and communicate the response to the whole group.
- Participate as fully as possible in the learning activities.
- Use the ‘hands up’ feature of Teams to indicate to the teacher that you wish to speak.
- You may not, at any time, record or take photos of your teacher of other participants during the video conference.