



# Acceptable Use of IT, the Internet and Electronic Communication including Social Media

<b>Committee Responsible:</b>	<b>Finance and Site</b>
<b>Reviewed by:</b>	Kieran Robinson and Paola Boyadjian
<b>Review Date:</b>	February 2025
<b>Ratified by Committee:</b>	4 <sup>th</sup> March 2025
<b>Next Review Date:</b>	February 2026

(We have merged our old IT policy with our new acceptable use policy (developed significantly in September 2024) and developed both in line with our practice)

<b>VERSION CONTROL</b>			
<b>Version</b>	<b>Date</b>	<b>Author/Reviewer</b>	<b>Substantive changes since the previous version</b>

# Contents

---

1. Introduction
2. Vision
3. Purpose and scope
4. Responsibilities
5. Disciplinary action
6. Training

## **SECTION 1 - Use of Bentley Wood High School IT resources**

7. Safe working practice
8. Loan of IT equipment
9. Health and safety guidance on using IT equipment including laptops
10. Use of trust/school IT equipment
11. Digital cameras
12. Software
13. Network access, passwords and data security
14. File storage
15. Monitoring of email

## **SECTION 2 - Electronic communications (including social media)**

16. Use of internet, email and other electronic communication
17. Social media
18. Access to social media at work for personal use
19. School social media accounts
20. Responding to online safety incidents and concerns
21. Working from home and remote access
22. Virtual meetings
23. Remote Learning
24. Safeguarding
25. Monitoring and review

## **Appendices**

Appendix 1 - Employee guidance on the use of social media (summary)

Appendix 2 - Additional guidance for headteachers on the use of social media

Appendix 3 - Acceptable Use Agreement - volunteers & visitors (model)  
*(to be personalised and adapted by each school to suit their requirements)*

Appendix 4 - Acceptable Use Policy & Agreement (model) - parents/carers & pupils  
*(to be personalised and adapted by each school to suit their requirements e.g. inclusion in home/school agreements and/or leaflets etc.)*

Appendix 5 - Device Loan Agreement for Pupils (model)  
*(to be personalised and adapted by each school to suit their requirements e.g. inclusion in home/school agreements and/or leaflets etc.)*

Appendix 6 - Device Loan Agreement for Staff (model)

---

## **1. Introduction**

---

- 1.0 Computers and other networked facilities, including internet access, are available to staff, pupils and some volunteers and visitors within schools.

This acceptable use agreement is designed to outline the responsibilities of the workforce including staff, volunteers, contractors and visitors when using technology (either personal devices or academy devices), both on and off Bentley Wood High School premises. This policy is part of our strategy to ensure that all members of our school community are safe and responsible users of technology.

- 1.1 All users must be aware of the Bentley Wood High School's policies and procedures relating to the use of IT resources. All adults and pupils connected to Bentley Wood High School need to understand their responsibilities concerning appropriate communication, safeguarding and data protection and must be conscious at all times of the need to keep their personal and professional lives separate.
- 1.2 A poorly administered network or weak password controls could expose the trust/school's information to an unauthorised user, introduce a virus or compromise data security resulting in a data breach. Pupils, parents and the public should have confidence in the trust/school's decisions and services.
- 1.3 This policy operates in conjunction with all relevant Bentley Wood High School policies.
- 1.4 This policy complies with the following legislation and guidance. It reflects legislation at the time when it was last reviewed. Any changes in legislation will take precedence over anything printed in the policy.
- [Data Protection Act 2018](#)
  - [The UK General Data Protection Regulation](#)
  - [Computer Misuse Act 1990](#)
  - [Human Rights Act 1998](#)
  - [The Telecommunications \(Lawful Business Practice\) Regulations 2000](#)
  - [Education Act 2011](#)
  - [Freedom of Information Act 2000](#)
  - [The Education and Inspections Act 2006](#)
  - [Keeping Children Safe in Education \(current version\)](#)
  - [Searching, screening and confiscation: advice for schools](#)

## **Definitions**

- 1.5 The "school" refers to Bentley Wood High School.
- 1.6 "Academy Data" or "Data" relates to data that is owned by Bentley Wood High School.
- 1.7 "Personal Devices" refers to any device that is not owned by Bentley Wood High School.
- 1.8 "Appropriate Person" refers to a staff member who has authority to grant permission for the area concerned.
- 1.9 "Staff" refers to any person who is undertaking work for the academy where email accounts and/or access to IT systems are provided for them to carry out their role. This includes but is not limited to, full and part-time staff, teaching students, volunteers (including governance roles) and apprentices.

## 2. Vision of IT in our School

---

“Bentley Wood High School aims to prepare IT/ learning infrastructures fit for the 21<sup>st</sup> 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:

- 2.0 To equip student with the skills necessary to learn outside the classroom over time to become lifelong learners.
- 2.1 Be fully aware of the risks and intelligence IT skills can bring to learning and their everyday lives.
- 2.2 To encourage students to become, develop a growth mindset philosophy, self-regulating their learning and empower them using IT as the keytool.
- 2.3 To provide appropriate opportunities for all students to acquire Computing skills throughout the curriculum;
- 2.4 To explore learner’s attitudes towards IT, its value for themselves, others and society;
- 2.5 To provide opportunities for students to work collaboratively locally and globally;
- 2.6 To promote the use of IT for inclusion purposes;
- 2.7 To implement a whole school high quality remote education if the circumstance requires i.e. school closure due to snow.
- 2.8 To effectively meet students' needs through the use of IT;
- 2.9 To provide staff development to improve teachers' IT skills;
- 2.10 To promote e-safety and provide educational support on wider IT issues;
- 2.11 To keep abreast of emerging technologies and evaluate the benefits for educational purposes.

All students regardless of race, gender or ability should have the opportunity to develop IT capability. We ensure that all our students:

- 2.12 have equal access to IT resources (including outside school);
- 2.13 have equal opportunities to develop IT capability;
- 2.14 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.

## 3. Purpose and Scope

---

- 3.0 This policy applies to all Bentley Wood High School staff (permanent and temporary), all governance roles, teacher trainees and other trainees, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school and/or the academy trust, ***collectively referred to as ‘staff’ in this policy.***
- 3.1 This policy sets out:

- the criteria for the acceptable use of Bentley Wood High School and/or school IT and communications system (e.g. PCs, laptops, tablets, mobile phones, wearable technology such as smartwatches etc.).
- the criteria for the acceptable use of social media and online communications both professionally and personally whilst working in or with the trust and/or school.

3.2 This policy is intended to ensure that:

- Bentley Wood High School's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- staff, volunteers, contractors, parents and pupils understand that their online conduct is their responsibility and must meet data protection and safeguarding requirements. Any personal or potentially personal information sent via e-mail and the internet is covered by the Data Protection Act 2018 and the provisions of the General Data Protection Regulation
- the confidentiality of pupils and other staff and the reputation of the school are safeguarded.

3.3 This policy is shared as part of the induction process for staff, regular volunteers and governors. It is shared each time there is an update. In the Autumn Term, all staff are required to confirm that they have read the policy and refreshed their knowledge of the contents (annual Safeguarding & Essential Policies Checklist).

## **4. Responsibilities**

---

4.0 Bentley Wood High School managers have a duty of care to all staff and to ensure that they have a reasonable work-life balance and that they work in a healthy and safe environment.

- Electronic ways of working should not place greater burdens on staff in terms of either workload or response times.
- Line managers will support any staff who are subject to abuse through any of the electronic media by effective and immediate sanctions, in the same way that it is expected that verbal and physical abuse is dealt with.
- Always think carefully about all forms of communication, but particularly electronic (which can be circulated widely and rapidly). If 'thinking about it' gives rise to any doubt, then the best advice is 'don't do it'.

4.1 All staff should understand filtering and monitoring systems in place within the school and that Bentley Wood High School and their IT service provider (AIT) may monitor the use of any Bentley Wood High School device and all internet use without additional notice.

4.2 Staff will ensure that they follow the requirements set out by data protection legislation and Bentley Wood High School policies when processing or storing data.

## **5. Disciplinary action**

---

5.0 Failure to follow the Acceptable Use of IT Policy could result in appropriate disciplinary action being taken, which may include a warning, suspension, dismissal from the trust/school and, in the case of illegal activities, referral to the police.

## **6. Training**

---

- 6.0 Staff will ensure they participate in any e-safety or online data protection training offered. It is mandatory for all staff to complete the GDPR training as part of the induction process before accessing personal data.
- 6.1 All staff and others accessing the trust's network will undertake Cyber Security Training as part of induction and annually thereafter.
- 6.2 Staff must understand that regular testing will be conducted periodically, without prior warning or notice, which may include phishing simulations or other similar activities. This may result in subsequent follow-up training for individuals

## **SECTION 1**

### **Use of Bentley Wood High School IT resources on or off school premises**

#### **7. Safe working practice**

---

- 7.0 All personnel must make careful, considerate use of the school IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.
- 7.1 Faulty equipment should either be reported promptly to the school office/IT coordinator who will report to the IT service provider (AIT) or directly to AIT via the Helpdesk ([help@advanceditservices.co.uk](mailto:help@advanceditservices.co.uk)) or 0115 9170197.
- 7.2 Personnel should immediately inform the school office/IT coordinator or the IT service provider (AIT) via the Helpdesk of any issues with devices, such as errors and alerts that may affect the security or function of the device.
- 7.3 Personnel should always be vigilant to identify emails that carry malware or phishing attempts and should:
- Not open attachments or click on links when content is not adequately explained
  - Check email and names of unknown senders to ensure they are legitimate before opening the email.
  - Look for inconsistencies or inappropriate style (e.g. grammar mistakes, capital letters, an excessive number of exclamation marks.)
- 7.4 If an individual is unsure that an email they have received is safe, they should request a check by our IT service provider via the school office/IT coordinator or directly to the AIT Helpdesk ([help@advanceditservices.co.uk](mailto:help@advanceditservices.co.uk)) or 0115 9170197.
- 7.5 Individuals are responsible for maintaining the security of computers and networks by using only their own log-on details and not allowing others to use their personal passwords.
- 7.6 Individuals should ensure that machines are not left unattended when they are logged on.
- 7.7 Individuals should ensure that when using work equipment at home, other family members do not use the equipment for their personal use.
- 7.8 Individuals are responsible for the security of all the content (software and data) on any trust-owned equipment allocated to them.
- 7.9 Hardware and software provided by the workplace for an individual's use can only be used by that individual and only for educational use or to serve the functions of the trust. Personal accounts or information such as personal photographs, files or financial information should not be accessed or stored on school devices and Bentley Wood High School accepts no liability for loss of such data.

Users must not attempt to bypass any filtering and/or security systems put in place by the school/trust

If staff or students discover unsuitable sites, the URL must be reported to the Network team;

- 7.10 Users must not remove or disable any software or systems implemented to ensure the security of trust/school-issued devices
- 7.11 Users should not install any unlicensed software on equipment allocated to them. Downloading or accessing programmes or files that have not been authorised could result in the activation of malware and ransomware when devices are reconnected to school networks. Where there is a resultant data breach, staff may be individually liable for such a breach and may face disciplinary action. If activities are illegal this will be referred to the police. If in doubt, staff should ask IT support for guidance.
- 7.12 Permissions and passwords should provide different access as appropriate to the user's role.

## **8. Loan of IT equipment and mobile devices**

---

- 8.0 Bentley Wood High School's IT equipment (e.g. laptop, tablet, mobile phone) is provided to users on a loaned basis and remains the property of the school. The school will ensure that users understand their responsibilities and will maintain a record of loans and returns.
- 8.1 Bentley Wood High School retains the sole right of possession of any school-owned device and may transfer the device to another user if users do not, or are unable to, for any reason, fulfil the requirements of this agreement.
- 8.2 The IT equipment provided must not be used by any persons other than the authorised user/s to whom it has been allocated and the property identification markings should not be removed for any reason.
- 8.3 No addition or deletion of any software or hardware is permitted without the express permission of the headteacher or IT Coordinator.
- 8.4 To ensure that security patches and virus definitions are up to date users should connect laptops to the school/trust network regularly.
- 8.5 All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, a laptop, tablet or mobile phone should never be left in a vehicle overnight or other unsecured, vulnerable situation. Any loss or damage to school/trust IT equipment should be immediately reported to the headteacher/line manager as this may constitute a data breach.
- 8.6 When employment or involvement with the school ends, users must return all computer equipment and software to the headteacher/line manager or school office staff in full working condition. The user account and all personal work stored on the laptop must be securely deleted and the user will be required to sign a confirmation that this has been done.
- 8.7 If software/hardware problems arise, a laptop or tablet may need to be restored to its original settings. Work files may be lost during the restore process. It is the responsibility of all users to ensure that backups of any documents stored locally on a device are regularly uploaded to the school networked server.
- 8.8 External hardware devices (e.g. USBs and external hard drives) are no longer permitted after Sept 2024 unless authority has been granted to use an encrypted hardware device by a senior manager following a written request with justification.
- 8.9 Where there is evidence that the laptop/tablet has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any laptop/tablet whilst on loan.



- 8.10 Where a laptop or tablet is loaned to parents/carers for the use of pupils e.g. during periods of remote learning, parents/carers must be informed of their responsibilities for the appropriate use and care of the equipment. When the loan period of the laptop or tablet ends, parents/carers must be required to return all computer equipment and software to the headteacher or school office in full working condition.
- 8.11 As part of safeguarding training, including induction training, expectations and responsibilities relating to filtering and monitoring will take place

The school reserves the right to oversee and monitor the activity of users on school networks, systems and school devices. The school uses Smoothwall Cloud filtering and monitoring systems to ensure both students and staff are safeguarded online (see Safeguarding policy). Our IT providers (AIT) may undertake checks on individual accounts as part of their IT monitoring responsibilities where concerns arise, e.g. inappropriate searches being detected, unusual data storage patterns. Access may be required for data protection purposes i.e. response to a Subject Access Request. We may need to check specific accounts if allegations of misuse have been made, or misuse is suspected.

Monitoring reports will be shared with the Governing Board as part of their annual schedule of business (see Safeguarding policy).

## **9. Health and Safety guidance on using IT equipment including laptops**

---

- 9.0 In the interests of health and safety, all users are advised to adhere to the following recommendations for the safe use of personal laptops. Any health and safety concerns associated with the use of laptops should be discussed with the headteacher. Further advice is available in the Bentley Wood High School Health & Safety policy.
- Sit in a chair that provides good back support to avoid backache and position the laptop/tablet directly in front of the user to avoid twisting;
  - Take regular breaks from the screen to reduce eyestrain.
  - Avoid using the laptop/tablet on a low table or the lap as both of these positions will increase strain on the neck and lower back.

## **10. Use of trust/school IT equipment**

---

- 10.0 Users who borrow IT equipment (laptops, mobile phones etc.) from the school must sign for it and take responsibility for its care. Loan equipment should be concealed and stored securely when not in use. Any loss or damage to equipment on loan should be immediately reported to the headteacher or IT Coordinator in the first instance, and any theft or criminal damage should also be reported to the police.
- 10.1 To prevent data loss and ensure consistent application of school policies no personally owned equipment should be attached to the school network without the permission of the headteacher of the relevant school. All mobile devices must be encrypted or password-protected wherever technology allows.
- 10.2 Users will only use school devices for school business unless special permission has been granted to use them for a personal purpose by a senior member of staff with the appropriate authority.

## **11. Software**

---

- 11.0 Users should use software in accordance with applicable licence agreements. To copy software or any supporting documentation protected by copyright is a criminal offence. The use

or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the trust. Under no circumstances should any user possess unlicensed software on school premises or use unlicensed software on trust/school IT equipment (including portable equipment).

- 11.1 No software may be added to the system or a device without the completion of a Data Protection Impact Assessment (DPIA) being undertaken. Please consult with the headteacher or a member of the school office staff.

## **12. Digital cameras, mobile devices and taking photographs**

---

- 12.0 Our schools encourage the use of school-owned digital cameras, mobile devices (e.g. iPads) and video equipment where appropriate and authorised to record events, activities and achievements. However, individuals should be aware of the following guidelines:
- Individuals must not use mobile devices to take images or videos of pupils unless an appropriate person has agreed to this.
  - Photos should only be named with the pupil's name if they are to be accessible in school only.
  - Photos for the website or press must only include the child's first name and parent's permission must be given prior to publishing.
  - All photographs/videos should be downloaded to the school network for storage
  - The use of personal mobile phones, digital cameras or wearable technology such as smartwatches for taking photographs/videos of pupils is not permitted.
  - At the discretion of the headteacher and subject to conditions, parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.
  - Individuals wishing to take photographs, video, or audio recordings in school **must** ensure that they are using a school-provided device e.g. camera, laptop etc.
  - Parental permission is not required to take photographs, films or recordings for the school's core purpose but consent must be sought and granted for any additional purposes (see Photography and Children's Images policy).
- 12.1 To protect the privacy of our staff, volunteers and pupils, and their safety and well-being, photographs, video, or audio recordings **must not** be published on blogs, social networking sites or disseminated publicly in any other way without the consent of all the people identifiable in them.
- 12.2 No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school.

## **13. Network Access, Passwords and Data Security**

---

- 13.0 Users must only access information held on the school's computer systems if properly authorised to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the school network or IT equipment be disclosed to unauthorised persons. If you accidentally access information which you are not entitled to view, report this immediately to the headteacher or school IT Coordinator.

- 13.1 Individuals using computers in classrooms must ensure that sensitive data is not accessible to students or other individuals by logging off or locking the computer as appropriate. In other areas, computers must not be left logged on when left unattended.
- 13.2 Passwords must be kept secure. System and administration level passwords should also be changed on a termly basis as a minimum.

Passwords should be complex and be at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- 13.3 All passwords are to be treated as sensitive, confidential information. Therefore, users must not:
- Write down passwords or store them online.
  - Use school user account passwords for other types of access
  - Reveal a password over the phone or in an e-mail message or other correspondence.
  - Talk about a password in front of others including family members.
  - Hint at the format of a password (e.g., "my family name").
  - Reveal a password on questionnaires or security forms.
  - Insert passwords into e-mail messages or other forms of electronic communication.
- 13.4 If an account or password is suspected to have been compromised, the incident must be reported immediately to the headteacher or school IT Coordinator so that the account password can be changed.
- 13.5 Visitors to a school must be granted permission by the headteacher or a senior member of staff to access the school Guest WiFi network. Authorisation will be granted if:
- Parents are working with the school in an official capacity (e.g. parent Governor).
  - Visitors need to access the wi-fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

### **External hardware devices**

- 13.6 External hardware devices (e.g. USBs and external hard drives) are no longer permitted after September 2024 unless authority has been granted to use an encrypted hardware device by a senior manager following a written request with justification.
- 13.7 Staff should clarify with the headteacher/data protection officer the nature of the material that may be held on these devices, for how long and with what security measures. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done with extreme care, following the trust's security protocol and using an encrypted memory stick provided by the trust/school, where required.

## **14. Data storage**

---

- 14.0 School data must be stored in accordance with the Bentley Wood High School Data Protection Policy and data protection legislation.
- 14.1 Each member of staff has a personal area on the school/trust network, as well as access to shared network drives.
- 14.2 Any school/trust related work should be stored on one of these network drives.
- 14.3 Personal files are not permitted on the network areas.

- 14.4 Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.
- 14.5 No school/trust data is to be stored on a home computer or external storage devices.
- 14.6 If accessing cloud files or email on personal device, it is the user's responsibility to ensure the device is password-protected and no data is stored on the device. Bentley Wood High School encourage an appropriate balance between school/work life commitment as part of managing wellbeing.
- 14.7 When processing school data on a personal device, individuals will ensure that the device is encrypted. The data will be subject to the data retention policy.
- 14.8 No confidential, or school data which is subject to the Data Protection Act should be transferred off-site unless it is sent by secure email or stored on an encrypted device.
- 14.9 Personal information about children which is no longer needed for a particular purpose should be deleted from the file (for example, group lists, test scores no longer needed) in accordance with the GDPR.

## **15. Monitoring of email**

---

- 15.0 Individuals will only use the approved email accounts or other forms of communication that have been provided and authorised by the school when conducting school business.
- 15.1 The school's email system automatically records details of all email sent both internally and externally. The automatic system highlights the use of certain prohibited words and any potential infringement will be referred to the headteacher as part of the routine monitoring procedures and may result in disciplinary action.
- 15.2 The following details are recorded in respect of every email message:
- name of the person sending the email,
  - the email addresses of all recipients and copy recipients,
  - the size and name of any file attachments,
  - the date and time sent,
  - a copy of the email,
  - a copy of file attachments.
- 15.3 The IT support provider (AIT) and an appropriate responsible person within the organisation may read and inspect individual emails and attachments for specific business/HR/legal purposes including:
- Establishing the content of transactions,
  - Ensuring users are complying both with the law and this policy
  - Checking email when staff are on leave, absent or for other supervisory purposes.
  - To respond to a Subject Access Request or Freedom of Information Request
- 15.4 The purpose for accessing emails must be clearly demonstrable.
- 15.5 Suspected misuse of the school's computer systems by users will be considered by the headteacher as appropriate.

## **16. Bring Your Own Device Policy (BOYD)**

---

- 16.0 Bentley Wood High School recognises that the use of personal devices by staff, visitors and volunteers (e.g. teaching students, healthcare professionals etc.) is a practical requirement in certain circumstances. This policy is designed to support the use of guest devices in schools where these supports working practices. It aims to protect children from harm, minimise risk to the school networks and explain what constitutes acceptable use.
- 16.1 The Bring Your Own Device (BYOD) policy applies to all use of guest devices to access the internet via the schools' guest network or to access school information, by staff or visitors. Guest devices include laptops, tablets, smartphones, USB sticks, wearable technology (including smart/apple watches) and any other device considered portable and/or with the ability to connect to Wi-Fi and the Internet which is not school-owned or on the school asset list, including staff personal devices.
- 16.2 The use of personal devices in school and access to the school networks is in accordance with school policies including the Acceptable Use of IT Policy, the Online Safety Policy (Including Filtering & Monitoring), the Data Protection Policy and the relevant Code of Conduct. Users of personal devices are required to be aware of the need to:
- Protect children from harm
  - Understand what constitutes misuse
  - Minimise risk from BYOD
  - Report suspected misuse immediately
  - Be responsible for their own professional behaviour
  - Respect professional boundaries

### **Access to the Trust's Internet Connections**

- 16.3 The school provides a guest wireless network connection that staff and visitors may, with permission, use to connect their own devices to the Internet. Guest devices (any device which is not school owned or on the school asset list) should only be connected to this guest network for access.
- 16.4 Permission must be sought before connecting any device to a school network. Access to the network is at the discretion of the school and the school reserves the right to refuse staff and visitors permission to use their own devices on school premises. The school may withdraw access from anyone it considers is using the network inappropriately.
- 16.5 The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk.
- 16.6 The school does not permit the downloading of apps or other software whilst connected to the school network and the school will not be held responsible for the content of any downloads onto a user's own device whilst using the school's network.
- 16.7 The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from the use of the school's network.
- 16.8 Staff and visitors are responsible for their own devices at all times. The school is not responsible for the loss, or theft of, or damage to a personal device or storage media on that device howsoever caused, including lost or corrupted data.
- 16.9 The school must be notified as soon as possible of any loss, or theft of a personal device that has been used to access school systems, and these incidents will be logged with the Data Protection Officer (DPO) and the school's IT support provider (AIT).

- 16.10 Data protection incidents should be reported immediately to the school's Data Protection Officer in accordance with the Data Protection Policy
- 16.11 Personal devices used to access school systems must enable automatic updates for security patches from the supplier. Applications installed on the device must also be subject to regular security updates and licensed.
- 16.12 The school cannot support users' own devices, nor is the school responsible for conducting annual PAT testing of personal devices.
- 16.13 Where the school uses Multi-Factor Authentication, personal mobile phones can be used to receive the necessary authentication code.
- 16.14 Where staff are permitted to connect to school IT systems from their own devices, a second layer of security should be enabled such as a password, and/or encryption must be in place and notifications must be turned off the lock screen. It is the responsibility of the owner of that device to ensure it is safe for the purposes for which they wish to use it.
- 16.15 Staff and visitors must **not** store personal data about pupils or others on a personal device, or cloud servers linked to personal accounts or devices.
- 16.16 Visitors in a professional capacity (e.g. medical personnel) who are using a device that is owned by the organisation they work for, may store information in the discharge of their professional duties and in accordance with their employing organisation's policies, procedures and data protection legislation
- 16.17 With permission, it may be necessary for staff/visitors to download school information to their own devices to view it (for example, to view an email attachment). Email attachments are the most common source of cyber-attacks. Please follow the guidance on cyber security and email protection and be aware that personal devices are not subject to the same security controls and safeguards that protect the school network and devices.
- 16.18 Any unauthorised access to, or distribution of, confidential information should be reported to the headteacher and the Data Protection Officer (via the school office) as soon as possible in line with the trust's data protection policies.
- 16.19 Before selling or gifting a personal device which has been used to access a school network to someone else it must be cleansed of all school related data, emails, systems and apps.
- 16.20 Staff/visitors must not send school information or personal data to/from their personal email accounts, social media or similar accounts.

### **Monitoring the use of personal devices**

- 16.21 The school reserves the right to use technology that detects and monitors the use of personal devices which are connected to or logged on to our wireless network or IT systems. The use of such technology is to ensure the security and appropriate use of the school IT systems and safeguard school information.
- 16.22 The information that the school may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.
- 16.23 Any inappropriate content received through school IT services or the school internet connection should be reported to the IT Support Service Provider (AIT) via the Helpdesk and the Designated Safeguarding Lead advised as soon as possible.

### **Security of staff/visitor personal devices**

- 16.24 Individuals must take all sensible measures to prevent unauthorised access to their own devices, including but not limited to the use of a PIN, pattern, face recognition or password to unlock the device, and ensuring that the device auto-locks if inactive for a short period. Individuals must ensure that appropriate security software is installed on their own devices and must keep the software and security settings up to date

**Permissible and non-permissible use**

- 16.25 Individuals participating in BYOD must comply with the Acceptable Use of IT Policy.
- 16.26 The headteacher has the right to locally enforce storage of staff or visitor devices in a secure location such as the school office.
- 16.27 The headteacher can decide if devices can or cannot be taken into areas around the school where there are particular safeguarding issues (such as changing rooms). In such cases, the school should agree with and inform staff and visitors which areas are expected to be "BYOD free". The headteacher can choose to refuse to allow any personal and/or mobile devices such as mobile phones or smartwatches to be used on site.
- 16.28 Visitors and contractors to the school/site should be informed of the policy regarding personal devices upon arrival.
- 16.29 Personal devices must not be taken into controlled assessments, unless special circumstances apply.
- 16.30 Staff, volunteers and contractors should not use their own devices (e.g. mobile phones) for contacting children and young people or parents/carers, unless it is an emergency and they are unable to use or access the school's IT systems. If it is necessary for a phone call or text to be taken or received, care should be taken to avoid disturbance or disorder to the running of the school.
- 16.31 Users must never attempt to bypass any security controls in school systems or their own devices.
- 16.32 This Acceptable Use of IT Policy sets out in further detail the measures to ensure responsible behaviour online.

## **SECTION 2**

### **Electronic communications, social media and online professionalism**

*(including email, social media and video conferencing for meetings and remote learning)*

#### **17. Use of internet, e-mail and other electronic communications**

---

- 17.0 Internet and email use are integral to the effective delivery of educational services provided by the school. Nothing in this policy should be read as restricting the proper use of email and the internet for trust/school activities.
- 17.1 Members of staff and some volunteers (e.g. trustees and governors) are provided with a school email address. The email system can be accessed from both the school computers and via the internet from any computer. All trust/school-related communication must be via the school email address wherever possible.
- 17.2 Email is not a confidential means of communication. There is no guarantee that electronic communications will remain private. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Once an email is transmitted it may be altered. Deleting or recalling an email will not eliminate it from computer systems outside of the computer network.
- 17.3 The burden of responsibility for the appropriate use of email lies with the sender of the message.
- 17.4 All personal data must be encrypted when sent using email or other insecure electronic file transfer methods. The level of security is dependent upon the type of sensitive data.
- 17.5 A basic level of security may be to password protect the document being shared via email and send the password to unlock the document via a different means of communication e.g. text



message. Please note: sending a password in a second separate email is NOT considered secure.

- 17.6 A more advanced level of communication security may be to use a secure encrypted File Transfer Process (FTP) or use the email encryption setting within the email client. i.e. Microsoft Outlook. Information on how to send secure files via FTP or using email client software such as MS Outlook can be provided by the IT service provider (AIT) using the Helpdesk.

### **Personal use of internet and email**

- 17.7 Staff and volunteers must not connect personal devices (e.g. a mobile phone) to the school internet connection for their personal use. Personal devices may be connected (with permission) in accordance with the BYOD policy (paragraph 15 above).
- 17.8 Individuals are not allowed to use school tablets/iPads for any personal internet activity as these are for education purposes and work-related research only.
- 17.9 Use of e-mail and the internet (including social media), which brings the trust/school into disrepute, may result in disciplinary action.
- 17.10 If your personal device is connected to the internet the school operates filtering/monitoring software which gives an overview of all browsing data.
- 17.11 Access to personal email accounts must only be in staff members' own time.
- 17.12 Staff/other individuals must not engage in social interaction using electronic means (e.g. through instant messaging or on social media) during working time or in the presence of pupils.
- 17.13 Staff and volunteers should be aware that any activity received/sent through the school network, is recorded and may be monitored.
- 17.14 School equipment should not be used to access the internet for trading or personal business purposes. Use of the internet to buy goods or services for personal use will not render the school liable for default of payment or the security of any personal information disclosed. Staff and volunteers should not use the school's computer system for making personal payments. Personal goods ordered to be delivered to work addresses should be agreed in advance with the school office staff.
- 17.15 The school's facilities must never be used for the passing of inappropriate personal information of any kind.

### **Email communications**

Staff should remain aware of their professional position when communicating via email.

Staff should take great care when emailing or responding to an email from a student. Staff should seek to end the email communication at the earliest possible time and continue that communication in person.

When email is used to communicate with parents, carers or any school business as part of a professional role, a school email address should always be used.

- 17.16 The style and format of any email communication should be strictly professional. Improper statements in email can give rise to personal liability and liability for the school and may constitute a serious disciplinary matter. Emails that embarrass, misrepresent or convey an unjust or unfavourable impression of the trust/school or its business affairs, staff, suppliers and their families are not permitted. Staff must not use e-mail in any way that is insulting or offensive.

- 17.17 Staff should consider whether it is advisable to copy a colleague into any contact with a parent as a further safeguard (subject to data protection considerations).
- 17.18 Staff are NOT permitted to communicate with pupils directly via non-school email.
- 17.19 Staff should be aware that email is not always the best form of communication and should consider alternatives, as appropriate.
- 17.20 Extreme care must be taken when using the school's email facilities to transmit information. Confidential or sensitive information should not be sent via the internet or email unless the data is protected by the trust/school's secure provision for such communications. Staff should remember that when a Subject Access Request or Freedom of Information request is submitted, relevant email communications will be included in the material to be provided.
- 17.21 In accordance with Data Protection legislation, emails should be deleted when they are no longer required for official records in accordance with the principle of data minimisation and the school's data retention policy which sets out the retention periods for the different categories of data.
- 17.22 Unless required as part of their role and with clear permission, staff must not deliberately view, download, upload or transmit any material that:
- could constitute bullying
  - is sexually explicit or obscene
  - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
  - contains material the possession of which would constitute a criminal offence
  - promotes any form of criminal activity
  - contains unwelcome propositions
  - contains images, cartoons or jokes that will cause offence
  - appears to be a chain letter

There should be no expectation, other than by agreement, that staff will be available outside normal working hours because they can access emails from home. There will therefore be no expectation, other than by agreement, that staff will respond to email or other messages, sent outside the working day, before the start of the next working day. This should be made clear to parents (see Home School Communications Policy).

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.

### **Internet access**

- 17.23 Many internet sites contain unacceptable content. Staff must not deliberately view, copy or circulate any material that:
- is sexually explicit or obscene
  - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
  - contains material, the possession of which would constitute a criminal offence
  - promotes any form of criminal activity

- contains images, cartoons or jokes that will cause offence
- that constitutes bullying

17.24 Staff must make every endeavour to protect pupils from harmful or inappropriate material accessible via the internet or transportable on computer media. Internet sites used for curriculum purposes must be checked by staff before lesson delivery.

### **Accidental Access to Inappropriate Material**

17.25 Many internet sites that contain unacceptable content are blocked automatically by the school's filtering systems. However, it is not possible to block all 'unacceptable' sites electronically in all circumstances. If staff become aware of any sites that require re-categorising they should inform the school IT Coordinator as soon as possible who will then inform the IT services provider.

17.26 Staff or pupils may receive an e-mail or visit an internet site that contains unacceptable material. If this occurs, a line manager or the headteacher should be informed as soon as possible. The staff member should ensure a short, written record is kept as they may be asked to provide details relating to the incident and an explanation of how it occurred. This information may be required later for management or audit purposes.

### **Copyright**

17.27 Staff may violate copyright law if text is simply cut and pasted into another document. This may equally apply to photographs and music samples used as illustration or backing tracks in resource materials. Teachers should make it clear to pupils that care should be taken when including this type of material in any schoolwork. Most sites contain a copyright notice detailing how material may be used. If in any doubt about downloading and using material for official purposes, legal advice should be obtained. Unless otherwise stated on the site all downloaded material must be for curricular or research purposes and must not be passed to third parties.

17.28 Downloading video, music files, games, software files and other computer programs for non-work-related purposes is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.

17.29 No software or apps should be downloaded for use without the prior permission of the headteacher as appropriate. All purchases of software or apps must have formal prior approval at the appropriate level of financial delegation. A Data Protection Impact Assessment must be conducted before any software or apps are utilised.

## **18. Social Media**

---

18.0 For the purposes of this policy, social media is defined as a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as X, Facebook, Instagram, LinkedIn, internet newsgroups, and chat rooms. Social media also covers blogs and video/image-sharing websites such as YouTube and Flickr. This is a constantly changing area. These guidelines should be followed in relation to any social media used.

18.1 As well as bringing many positive benefits, there are also many potential problems in utilising social media, both professionally (e.g. school X account) and personally (e.g. Facebook or Instagram account). Online conduct can have an impact on the role and reputation of staff members.

The following guidance is given to all staff and volunteers for their protection. The guidance should apply whether the individual is using trust/school equipment or their own equipment. The personal use

of social networking sites using trust/school equipment is not permitted on school premise, unless authorised by the Headteacher for school purposes.

- 18.2 At all times, staff and volunteers (including trustees and governors) should behave in accordance with the code of conduct expected of professional adults working with children. All staff are expected to behave appropriately and responsibly and should be aware that they may be accountable to the trust/school for actions outside of their work.
- 18.3 Safe and responsible use of social media will be discussed with all members of staff as part of induction and revisited regularly.
- 18.4 Many staff will use social networking outside of work to keep in touch with family, friends or activity groups. There will clearly be occasions when contacts within these situations result in links between staff and pupils at a school (for example being 'friends' with a parent of a pupil). Staff should try to ensure that in such circumstances they can make a professional distinction between their role as a 'friend' outside work and their role within work.
- 18.5 Staff who work directly with members of the public, including parents, need to be aware that the information they post on social media can make them identifiable to members of the wider school community as well as people they know in a private capacity. Staff should therefore consider this when setting up a profile, particularly in relation to the use of a photograph and/or providing details of their occupation, employer and work location. Online sites such as Facebook are in the public domain, and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Also, if a user's profile is linked to other sites, any changes to their profile will be updated there too. Staff/volunteers who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard and therefore comments, photographs or video clips sent to such contacts may be more widely available than originally anticipated. Staff must be aware that disgruntled parents or member of the community could 'tag' their account to issues that they believe exist in school (e.g. bullying). The school/trust will advise a personal referral to the police and social media platform administrators in the event of such an occurrence.
- 18.6 Staff and volunteers should consider very carefully any potential conflict of interest that could arise when linking through social media to people they also know through work/their role in the trust/school. The trust considers it inappropriate to have pupils as 'friends' through social media, and consequently, to do so may be considered to be a disciplinary matter.
- 18.7 Staff will not accept "friend requests" from any parents over personal social networking sites unless the person is known outside of their job role.
- 18.8 All staff should be aware of the image they are presenting when communicating via social media and ensure, as far as possible, that any comments made are not open to misinterpretation. Circulation of comments on social media can be rapid and widespread and therefore staff should be encouraged to adopt the general premise of not putting anything on such a site (or in an email) that they would not put in a formal letter, be prepared to say in a face-to-face conversation or discuss in a public place.
- 18.9 Staff representing the trust/school online, e.g. through blogging or on a school/trust social media account, will express neutral opinions and will not disclose any confidential information regarding the trust/school, or any information that may affect its reputability, unless otherwise directed.
- 18.10 Any information published online can be accessed around the world within seconds and will be publicly available for all to see, and is not easy to delete/withdraw once published. The trust/school views any comment that is made on a social media site as made publicly, and that any inappropriate comment made, will be considered in the context of which it is made. Staff

are advised to be mindful that nothing on a social media site is 'private' so comments made must still meet the standards of the role-specific code of conduct and other relevant policies.

- 18.11 Staff may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of trust/school policies, impacts on or compromises the staff member's ability to undertake their role, or undermines management decisions. Such behaviour would be investigated and may result in disciplinary action being taken, and could result in dismissal.
- 18.12 The school/trust views any comment that is made on social media to, potentially, have been made publicly. However, any inappropriate comment be considered in the context in which it is made. Members of staff should inform the headteacher if they consider any content shared on a social media site potentially conflicts with their role.
- 18.13 Whilst generic political discussion is not to be discouraged, staff must not participate in discussions that may bring the trust/school into disrepute and not give information or advice that they know to be contrary to trust/school policies or interests. Staff should not engage in chat which would embarrass, misrepresent or convey an unjust or unfavourable, impression of the trust/school or its business affairs, staff, suppliers, pupils or their families. Staff should remember these sites are public forums.
- 18.14 Any communications that staff make through social media must not:
- bring the trust/school into disrepute, for example by:
    - criticising, disagreeing or arguing with parents, colleagues or managers
    - making defamatory comments about individuals or other organisations/groups;
    - posting images that are inappropriate or links to inappropriate content;
  - breach confidentiality, for example by:
    - referring to confidential information about an individual (such as a colleague or pupil) or the trust/school
  - do anything that could be considered discriminatory against, or bullying or harassment of, any individual or group of individuals, and in contravention of trust/school policies, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual (such as the staff of the organisation), or posting images that are discriminatory or offensive or links to such content.
  - take other action that impacts on the employee's ability to do their job, for example by
    - online activity that is incompatible with the position they hold in the trust/school
    - any breach occurring inside or outside the workplace that is likely to affect the employee doing his/her work.
  - contravene trust/school policies, for example;
    - the relevant code of conduct, the anti-bullying policy, or the equality & diversity policy.

- 18.15 The school strongly recommends to all staff that personal interactions on social media sites do not include any reference to your work.
- 18.16 The above examples are not a definitive list of the misuse of social media but are examples to illustrate what misuse may look like.
- 18.17 Staff should use common sense when posting items; think about the intended audience and the consequences of making unwise remarks about colleagues, pupils or the school and its wider stakeholders. No sensitive or confidential information relating to the trust/school must be revealed on social networking sites.
- 18.18 Staff should be aware of the potential risks of communicating with ex-pupils in ways which may be considered inappropriate – particularly if it could be shown that the adult-pupil relationship of trust had been breached.
- 18.19 Staff should report any inappropriate contact from pupils or parents/carers to a member of the Senior Leadership Team at the earliest opportunity to prevent situations from escalating.
- 18.20 Staff are reminded that, as a safeguarding issue, they should always be careful about who they are ‘talking to’. It is very easy to hide identity in an online conversation.
- 18.21 Staff are reminded that they have a responsibility to report any racist, sexist or other discriminatory comments they become aware of through postings or chat on such sites.
- 18.22 In summary, staff are advised to safeguard themselves and their privacy when using social media sites. Areas of which to be mindful:
- Setting the privacy levels of personal sites
  - Being aware of location-sharing services
  - Opting out of public listings on social networking sites
  - Logging out of accounts after use
  - Keeping passwords safe and confidential
  - Not representing personal views as those of the school.
- 18.23 There can be particular issues for those new to the profession relating to the use of social network sites. It is likely that throughout their training period, they will have been regular users of such sites and have possibly been less concerned about the content of their ‘pages’ or the image they have presented of themselves. As part of their induction, they should be made aware of the issues raised above as a matter of priority and be advised to remove any material from such sites that may harm their new professional status. As many early career teachers maybe not much older than some of the pupils they will be working with, they must be made aware at a very early stage of the potential problems (including loss of job) that inappropriate comments and contact on social network sites (even if outside working hours) can cause.
- 18.24 Staff should be aware that all comments made through social media must meet the standards of the relevant legislation and regulations, including data protection legislation (the UK GDPR) and the expectations of staff conduct as expressed in the school’s policies for the management of Human Resources.

## **19. Access to social media at work, for personal use**

---

- 19.0 Staff are not allowed to access social media websites for personal use from the school’s computers or devices or their own personal devices (e.g. mobile phones and wearable technology such as smart watches) during working hours (contact time for teachers and teaching assistants), and they must not be left running “in the background”, whilst at work.

- 19.1 Leaving social media sites 'running' constantly in work time is considered to be a breach of the acceptable use policy, and would be considered to be using school resources for personal use, in work time, and as such would be investigated under the Disciplinary Procedure. These provisions also apply to personal computers and mobile devices.

## **20. School social media accounts**

---

- 20.0 Staff who have not been authorised to manage, or post to, Bentley Wood High School social media account (e.g. X) must not access, or attempt to access the account.
- 20.1 Those who are authorised to manage the account must ensure they abide by the guidelines in this policy and any specific policy related to the account, at all times.
- 20.2 Members of staff who follow and/or like the trust or school official social media channels are advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

## **21. Responding to online safety incidents and concerns**

---

- 21.0 All members of the school community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth-produced sexual imagery (sexting), cyberbullying and illegal content.
- 21.1 All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- 21.2 If staff believe any misuse or policy breach has occurred, they will inform an appropriate person (e.g., the line manager or the Designated Safeguarding Lead) providing full details of the misuse. If appropriate, please refer to the Bentley Wood High Whistleblowing Policy. Information provided will always be held in the strictest confidence.
- 21.3 Parents, carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure. We require staff, parents, carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include contacting the police, calling either 101 about a concern, or 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the Designated Safeguarding Lead/headteacher will speak with the Local Authority Safeguarding Team.

### **Dealing with inappropriate references to the school or staff**

- 21.4 Staff and volunteers etc. who find that 'friends' have posted inappropriate material relating to themselves on a social media site, should consider asking them and the site to remove it. They should also consider informing the headteacher (as appropriate) if there is the potential for repercussions for the school/trust.
- 21.5 If you find yourself the target of complaints or abuse on social networking sites you can take action yourself by using the mechanisms to report abusive activity. Most sites also provide some support for users who are subject to abuse. Again, it is advisable to let the headteacher know so you can benefit from their support.
- 21.6 If you find inappropriate references to you or the school posted by parents, colleagues, pupils or other members of the community, it is very important that you report this to the headteacher

as soon as possible. Do not attempt to address the situation yourself. The headteacher will then respond to the situation and ascertain your support needs.

- 21.7 All staff have a professional duty to report any knowledge of colleagues posting inappropriate content on social media which would breach the guidance contained above.

## **22. Working from home and remote access**

---

- 22.0 Staff may need to access personal data about other staff and pupils when working remotely, including when managing online learning.

Staff will access personal data on secure cloud service, so they do not need to keep any data on their devices

- 22.1 Staff accessing the school's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's IT facilities outside the school and take such precautions as the IT provider may require from time to time against importing viruses or compromising system security.

- 22.2 Wherever possible, devices will be provided by the school, so that appropriate security arrangements are in place. Whether using school equipment or personal equipment, staff should ensure that:

- The device is password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Wherever possible the hard drive is encrypted - this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Make sure the device locks if left inactive for a period of time
- Do not share personal devices you use for work purposes with family or friends
- Antivirus and anti-spyware software are kept up-to-date

## **23. Virtual meetings**

---

- 23.0 Staff (including governance roles) working from home or unable to meet physically may make use of virtual meetings using apps such as Microsoft Teams. All users must be aware of safeguarding and data protection considerations when making use of these applications and ensure that:

- They are made aware of and follow specific security guidance related to the use of the chosen application
- They attend meetings with the webcam/video switched on where possible
- They prevent unauthorised individuals from overhearing conversations (for example, by using headphones)
- They are mindful of their surroundings and consider the privacy of the room, including, but not limited to, who or what is visible or audible in the background

## **24. Remote learning**

---



- 24.0 Remote learning will only take place using the school/trust approved systems. Staff will only use Bentley Wood High School managed or specific, approved professional accounts with learners and/or parents/carers. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
- 24.1 Staff will only use Bentley Wood High School provided equipment and software for delivery of remote learning.
- 24.2 All remote lessons will be formally timetabled. Online contact with learners and/or parents/carers will not take place outside of the operating times set by the headteacher.
- 24.3 Live-streamed remote learning sessions will only be held with approval and agreement from the headteacher.
- 24.4 Live-streamed remote learning sessions may be recorded with the consent of the headteacher and those taking part. Consent for recording and storage will be sought from parents as part of each school's Remote Learning provision. There must be a clear purpose for making the recording and this should be made clear to parents/participants (e.g. safeguarding considerations) and arrangements for storage (how the recording will be stored, length of time and access) must be specified in accordance with data protection legislation.
- 24.5 Any personal data used by staff when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
- 24.6 A record of the length, time, date and attendance of any sessions held will be created. This will be stored securely as part of attendance records in line with the data protection policy. This is done automatically as part of MS Teams and does not need to be recorded or stored separately.
- 24.7 Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
- disabling/limiting chat
  - staff not permitting learners to share screens
  - use of waiting rooms/lobbies or equivalent.
- 24.8 When live streaming with pupils:
- contact will be made via school/setting provided email accounts and/or logins or via a parent/carer's account.
  - staff will mute/disable learners' videos and microphones as appropriate
- 24.9 Live sessions will be made available between the teacher and a group of children to talk to staff and share achievements/issues with work. These may be recorded and stored on school equipment as protection for staff should there be an allegation of inappropriate behaviour. The staff member will always be the last to leave the meeting.
- 24.10 Live 1:1 sessions with pupils will only take place with approval from the headteacher and parental agreement. A parent/carer is required to be present in the room.
- 24.11 A pre-agreed invitation/email detailing the session expectations will be sent to those invited to attend. Access links should not be made public or shared by participants.
- 24.12 Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
- 24.13 Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom. All participants are expected to behave in-line with existing school/setting policies and expectations. This includes:

- appropriate language will be used by all attendees.
- staff will not take or record images for their personal use.
- staff and attendees will wear appropriate dress.
- ensuring backgrounds of videos are neutral (blurred if possible).
- ensuring that personal information and/or unsuitable personal items are not visible, either on-screen or in video backgrounds.

- 24.14 Staff will remind attendees of behaviour expectations and how to report concerns at the beginning of the session.
- 24.15 If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the headteacher.
- 24.16 Inappropriate online behaviour will be responded to in line with the appropriate school policies. Sanctions for deliberate misuse may include:
- restricting/removing use
  - contacting the police if a criminal offence has been committed.
- 24.17 Any safeguarding concerns must be reported to the school's Designated Safeguarding Lead, in line with the school's child protection and safeguarding policy.
- 24.18 A useful reference source for protocols for Remote Working is the: [DfE guidance on Safeguarding & Remote Education](#)

## **25. Disclosures**

---

- 25.0 With the increased access of both pupils and staff to electronic communication, there is an increased chance of a disclosure being made to a member of staff through such a medium. Such a disclosure may be made outside normal working hours. The member of staff must follow the normal school procedures for reporting a disclosure as soon as they access the disclosure. This is set out in the child protection and safeguarding policy.

*(A further useful reference source is the booklet "Guidance on Safer Working Practice for Adults Who Work with Children and Young People")*

## **26. Monitoring and review**

---

This policy and procedure will be reviewed annually or whenever a change in legislation or practice necessitates a review, whichever is sooner.

The school will endeavor 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.

# Appendices

## Employee guidance on the use of social media (summary)

- Staff must be mindful that any online activities/comments made in a public domain, must be compatible with their position within the school/trust, and safeguard themselves in a professional capacity.
- Protect your own privacy. To ensure that your social network account does not compromise your professional position, ensure that your privacy settings are set correctly. Remember to upgrade access settings whenever the application/programme is upgraded.
- When setting up your profile online consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details. Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be “private” may still be in contravention of the school/trust’s HR Policies. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.
- Do not discuss work-related issues online, including conversations about pupils, parents, complaints, management or disparaging remarks about colleagues or the school. Even when anonymised, these are likely to be inappropriate. In addition, doing this in the presence of others may be deemed as bullying and/or harassment.
- Do not under any circumstances accept friend requests from a person you believe could be a student/parent or may conflict with your employment.
- Be aware that other users may access your profile and if they find the information and/or images it contains offensive, complain about you to the school as your employer.
- Ensure that any comments and/or images cannot be deemed defamatory, libellous or in breach of copyright legislation.
- You can act if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and support users who are subject to abuse by others.
- If you find inappropriate references and/or images of you posted by a ‘friend’ online you should contact them and the site to have the material removed. It would be wise to alert your friends in advance to the implications for you, as a school employee, of posting material related to you.
- If you find inappropriate references to you posted by parents, colleagues, pupils or other members of the school community, report this to the headteacher.
- If you are concerned about someone’s behaviour online, you should take steps to raise your concerns. If these are work-related you should inform your headteacher/DSL.
- Staff should also act in accordance with the all the school human resources policies and Child Protection/Safeguarding policies.
- Staff should not access social media sites or leave these running in the background during working hours (contact time for teachers and teaching assistants).

## Additional guidance for headteachers on the use of social media

### Headteachers are responsible for:

- Remaining familiar with this policy and the employee guidelines for using social media summarised in Appendix 1.
- Keeping up-to-date with relevant legislation and safeguarding issues regarding the use of social media.
- Ensuring staff and volunteers are made aware of the policy, guidelines and provided with appropriate training/briefing on induction and at regular intervals.
- Taking prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not, including taking steps to seek the prompt removal of any inappropriate material.
- Making parents and pupils aware of the implications of posting comments about the school and members of the school community. Details should be included in the Home School Agreement and/or school brochure to indicate the appropriate means for parents to raise concerns. It is advised that these documents also refer to the potential implications of posting inappropriate comments about the school/staff/pupils/wider community members. The agreement should also warn against the unauthorised taking of photographs of staff and/or making sound recordings.
- Supporting employees who are the subject of abuse, through existing policies and procedures.
- Ensuring all complaints and allegations are dealt with fairly, consistently, and in accordance with other employment policies where appropriate.

### Headteachers will:

- Ensure staff are advised of this policy on appointment and discuss during induction so that they are fully aware of its content.
- Remind staff on an annual basis of the guidance on the use of social media.
- Ensure staff are aware of how to raise concerns
- Include in the relevant section of the Information and Communication Technology curriculum, advice for pupils on the safe use of social media, the restrictions on use of these media for contact with school staff and the implications of posting material on such sites.
- Provide guidance for parents in supporting their children's safe use of social media
- Include in documents like the school brochure and home/school agreement, the school's approach to the taking of photographs of pupils, by the school or by parents, and how these may be used. Seeking parents' agreement at the outset and alerting them to potential pitfalls is likely to reduce issues of concern occurring. Parents may need to be made aware of the potential consequences of posting pictures on social media which include children other than their own, without parents' permission.
- Ensure parents and pupils are made aware that the use of social media to make inappropriate comments about staff, other parents or pupils will be addressed by the school in the same way as if

these remarks were made in person, in the public domain. Outline how such actions are likely to be damaging to the smooth running of the school and therefore the delivery to children.

- Respond quickly to those posting inappropriate comments. You may wish to issue a standard letter from the chair of governors asking them to contact the school/named person on a specific number. When following up, direct them to the appropriate processes for addressing issues or lodging complaints. Ensure the school's actions demonstrate both that harassment will not be tolerated and that expressing concerns through appropriate channels will ensure they are taken seriously.

## Acceptable use of IT, the internet and electronic communication

### VOLUNTEERS AND VISITORS

(who are provided access to the school's IT facilities)

**Name:**

When using the school's IT facilities and accessing the internet in school, or outside the school on a work device, I will follow the Acceptable Use of IT policy and I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the trust/school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the trust/school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the trust/school

- I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems using Filtering and Monitoring technology. This may include email communications.
- I will take all reasonable steps to ensure that work devices or personal devices that I use for school/trust communications and business are secure and password-protected ~~when using them outside school~~, I will keep all data securely stored in accordance with this policy and the trust's data protection policy.
- I will let the designated safeguarding lead (DSL) and headteacher know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's IT systems and internet responsibly and ensure that any pupils in my care do so too.

**Signed:**

**Date:**

# Acceptable Use of IT, the internet and electronic communication

## PUPILS & PARENTS

At Bentley Wood High School we take the safety of our pupils both in and out of school very seriously.

Within school, all children are taught about how to stay safe online and how to report incidents.

Our Remote Learning provision may require some online interaction between pupils and parents at home and teachers providing lessons and guidance on learning.

Please note that because of your child attends Bentley Wood High School, it is an expectation that you and your child are agreeing to abide by the school's policies. Please see the home/school agreement for further information.

## Parents

1. Online channels are an important way for parents/carers to communicate with, or about, our school.
2. Parents/carers may also set up independent channels to help them stay on top of what's happening in their child's class. For example, Facebook groups, email groups, or chats (through apps such as WhatsApp). These are not monitored or managed by the school.
3. When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:
  - Be respectful towards members of staff, and the school, at all times
  - Be respectful of other parents/carers and children
  - Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's social media (e.g. Facebook etc.), or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's social media (e.g. Facebook etc.), or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers
- Seek to "friend" staff working at the school on social media (unless I have a personal friendship)



4. I understand that if I am provided with access to a school learning platform where posting or commenting is enabled I will abide by any additional acceptable use requirements that are provided as a condition of use.
5. I understand that if I am provided with access to a live video link for the purposes of my child's remote learning or meetings with teaching staff, I will abide by any additional acceptable use requirements that are provided as a condition of use. For example:
  - I will not record or capture images of staff.
  - I will be respectful and behave appropriately at all times
  - I will report any concerns to the headteacher immediately
6. I understand that my child's safe use of the internet and online technologies outside of school is my responsibility

## **Pupils**

### **For my own personal safety in school and at home:**

- I understand that the school will monitor my use of IT in school.
- I will keep school usernames and passwords safe and secure. I will not share my password. I will not use anyone else's password (even with their permission).
- I will be aware of "stranger danger" when I am communicating online.
- I will not share personal information about myself or others when online without telling an adult first (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, photos etc.)
- I will tell a trusted adult if anything I see online makes me feel uncomfortable or upset.
- I will never answer unpleasant, suggestive or bullying emails or messages and I will always report them to a teacher or parent. I will not delete them straight away. I will show them to the person I have reported to, as evidence.

### **I understand that everyone has equal rights to use technology as a resource and:**

- 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 from a member of staff.
- I will not use the school systems or devices for online gaming or video broadcasting, unless I have permission from a member of staff.
- I will not use a memory stick from home in a school computer.

### **I will act as I expect others to act toward me:**

- I will respect other pupils' work and property and I will not access, copy, remove or otherwise alter anyone else's files without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I appreciate that others may have different opinions.
- I will not take photographs or share pictures of anyone without their permission.

### **I understand that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

- 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. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I understand that my use of the school's internet and IT is monitored by the Bentley Wood High School IT service provider and the school/ and will be subject to regular checks.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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.
- I will not install, or attempt to install or store, programmes of any type on any school device. I will not try to alter computer settings.
- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school. *The majority of these are filtered out by the school's filtering system.*

**When using the internet for research or recreation, I understand that:**

- I should ensure that I have permission to use the original work of others in my work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- 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.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school and where they involve my membership of the school community (*examples would be cyber-bullying another member of the school community, use of images or personal information of another member of the school community, posting threatening /offensive comments regarding another member of the school community*).
- Remember with social media, when you type something it's always there and you can't take it back. So be careful of what you say and write.
- I understand that if I fail to comply with this IT usage agreement, I may be subject to disciplinary action. This may include:
  - loss of access to the school network/internet
  - contact with parents
  - exclusion
  - in the event of illegal activities - involvement of the police.

**MS Teams – Remote Learning Code of Conduct:**

I understand that by joining remote learning live sessions I agree to follow the code of conduct outlined below:

- I understand that while online, I must behave the same way as I am expected to behave in school.

- I will make sure that my communication online is always supportive of my learning and the learning and wellbeing of others. I will communicate in a respectful way at all times.
- During live online sessions, my parent/carer will be near me (in the room or a nearby room with the door open).
- I will end sessions when the teacher tells me to do so.
- When taking part in an online session I will make sure that my environment is quiet and free from distractions, and the background is appropriate (check what is visible behind you).
- I will ensure that I am suitably dressed (fully dressed and not in pyjamas!).
- I will remain attentive.
- I will sign into MS Teams every day to help ensure that I keep on track with my learning.
- I will not take photos of my screen or record online interactions.
- At the end of live meetings my teacher will ask me to 'hang up' before closing the meeting. I will do this promptly as directed by my teacher.
- I understand that online sessions will be recorded by my teacher but that the recordings will not be made public.
- I understand that should I fail to follow this Code of Conduct, my teacher will remove me and contact my parents.

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

<b>Pupil's full name:</b>	
<b>Parent's full name</b>	
<b>Parent's signature</b>	

# Device Loan Agreement for Pupils and Parents

---

## Part 1 - Agreement

One copy for parent/carer and one copy to be retained in school

### **This agreement is between:**

Bentley Wood High School and the parent/carer of the student governs the use and care of devices assigned to the parent's child (the "pupil"). This agreement covers the device from the date it is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

The school is lending the pupil a laptop ("the equipment") for the purpose of doing schoolwork at school and at home.

This agreement sets the conditions for taking a Bentley Wood High School laptop] ("the equipment") home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of the loan.

## 1. Damage/loss

- a. By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.
- b. I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.
- c. If the equipment is damaged, lost or stolen, I will immediately inform the headteacher and I acknowledge that **I am responsible for the reasonable costs requested by the school to repair or replace the equipment.** If the equipment is stolen, I will also immediately inform the police.
- d. I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.
- e. I will not leave the equipment unsupervised in unsecured areas.
- f. I will make sure my child takes the following measures to protect the device:
  - i. Keeps the device in a secure place when not in use
  - ii. Does not leave the device in a car or on show at home
  - iii. Does not eat or drink around the device
  - iv. Does not lend the device to siblings or friends
  - v. Does not leave the equipment unsupervised in unsecured areas

## 2. Unacceptable use

- a. I am aware that the school and the school's IT service providers monitor the pupil's activity on this device.
- b. I agree that my child will not carry out any activity that constitutes 'unacceptable use'. This includes, but is not limited to the following:
  - i. Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination

- ii. Any illegal conduct, or statements which are deemed to be advocating illegal activity
- iii. Activity which defames or disparages the school, or risks bringing the school into disrepute
- iv. Causing intentional damage to IT facilities or materials
- v. Using inappropriate or offensive language
- c. My child will abide by the school's Acceptable Use of IT policy.
- d. I accept that the school will sanction the pupil, in line with our behaviour/discipline policy, if the pupil engages in any of the above at any time.

### 3. Personal use

I agree that the pupil will not use the equipment inappropriately and will not loan the equipment to any other person. While at home I accept that as the parent/carer I am responsible for monitoring my child use of the device.

### 4. Data protection

I agree to take the following measures to keep the data on the device protected.

- a. Keep the equipment password-protected - strong passwords are at least 8 characters long, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- b. Make sure my child locks the equipment if it's left inactive for a period of time
- c. I will not share the equipment among family or friends
- d. If I need help doing any of the above, I will contact the school.

### 5. Return date

- a. I will return the device in its original condition to the school office within 5 working days of being requested to do so.
- b. I will ensure the return of the equipment to the school if the pupil no longer attends the school.

### 6. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

<b>Pupil's full name:</b>	
<b>Parent's full name</b>	
<b>Parent's signature</b>	

### Part 2 - Record of loan

To be filled out by staff signing out/receiving the equipment. **To be retained in school.**

Details of pupil	
Pupil Name	
Year & Class	
Parent's Name (who signed the agreement):	
Loan details	
Date of Issue	
Equipment Details	
Type	
Make	
Model	
Serial Number	
Replacement Value	
Equipment Condition	
Accessory Details	
Description	Quantity
Equipment Return	
Date Returned	
Equipment returned in original condition?	<p style="text-align: center;"><b>Yes</b>                      <b>No</b></p>
<b>Comments if not in the original condition:</b>	

# Device Loan Agreement for Pupils

---

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I will adhere to the terms of the loan.

## Damage/loss

- I understand that I am responsible for the equipment.
- I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.
- I will make sure I will protect the device by:
  - Keeping the device in a secure place when not in use
- Not eating or drinking around the device
  - Not damaging the device intentionally
  - Does not lend the device to siblings or friends
  - Does not leave the equipment unsupervised in unsecured areas
    - If I do not look after the device by following the steps set out in C I acknowledge that **my family may be responsible for the reasonable costs requested by the school to repair or replace the equipment.** If the equipment is stolen, my family will also immediately inform the police and school.

## Unacceptable use

- I am aware that the school can monitor your activity on this device at school and at home.
- I agree not to use the laptop for any activity that constitutes 'unacceptable use'. This includes, but is not limited to the following:
  - Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
  - Any illegal conduct, or statements which are deemed to be advocating illegal activity
  - Activity which defames or disparages the school, or risks bringing the school into disrepute
  - Causing intentional damage to IT facilities or materials
  - Using inappropriate or offensive language
  - You agree to follow the school's Acceptable Use of IT policy.
- I accept that the school will sanction me if I engages in any of the above at any time.

## Data protection

- I agree to take the following measures to keep the data on the device protected.
  - Keep the equipment password-protected - strong passwords are at least 8 characters long, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
  - Make sure the device is locked if the equipment if it's left inactive for a period of time
  - I will not share the equipment among family or friends
  - If I need help doing any of the above, I will contact the school.

## Return date

- I will return the device in its original condition to the school office within 5 working days of being requested to do so.

**For my own personal safety in school and at home:**

- I understand that the school will monitor my use of IT.
- I will keep school usernames and passwords safe and secure. I will not share my password. I will not use anyone else's password (even with their permission).
- I will be aware of "stranger danger" when I am communicating online.
- I will not share personal information about myself or others when online without telling an adult first (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, photos etc.)
- I will tell a trusted adult if anything I see online makes me feel uncomfortable or upset.
- I will never answer unpleasant, suggestive or bullying emails or messages and I will always report them to a teacher or parent. I will not delete them straight away. I will show them to the person I have reported to, as evidence.

**I understand that everyone has equal rights to use technology as a resource and:**

- 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 from a member of staff.
- I will not use the school systems or devices for online gaming or video broadcasting, unless I have permission from a member of staff.
- I will not use a memory stick from home in a school computer.

**I will act as I expect others to act toward me:**

- I will respect other pupils' work and property and I will not access, copy, remove or otherwise alter anyone else's files without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I appreciate that others may have different opinions.
- I will not take photographs or share pictures of anyone without their permission.

**I understand that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

- 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. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I understand that my use of the school's internet and IT is monitored by Bentley Wood High School and will be subject to regular checks.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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.
- I will not install, or attempt to install or store, programmes of any type on any school device. I will not try to alter computer settings.
- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school. *The majority of these are filtered out by the school's filtering system.*



**When using the internet for research or recreation, I understand that:**

- I should ensure that I have permission to use the original work of others in my work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- 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.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school and where they involve my membership of the school community (*examples would be cyber-bullying another member of the school community, use of images or personal information of another member of the school community, posting threatening /offensive comments regarding another member of the school community*).
- Remember with social media, when you type something it's always there and you can't take it back. So be careful of what you say and write.
- I understand that if I fail to comply with this IT usage agreement, I may be subject to disciplinary action. This may include:
  - loss of access to the school network/internet
  - contact with parents
  - exclusion
  - in the event of illegal activities - involvement of the police.

**Consent**

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

<b>Pupil's full name:</b>	
<b>Date:</b>	
<b>Parent's signature:</b>	

## Device Loan Agreement for Staff

---

### Part 1 - Agreement

One copy for the staff member and one copy to be retained by the trust/in school

#### **This agreement is between:**

Bentley Wood High School and the employee and governs the use and care of devices assigned to individual staff members. This agreement covers the device from the date the device is issued through to the return date of the device to the school/trust.

All issued equipment shall remain the sole property of the school and is governed by the school policies.

The school is lending the employee an IT device ("the equipment") for the purpose of working from school and home, fulfilling work-related tasks, and/or a special project.

This agreement sets the conditions for taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

### 7. Damage/loss

- a. By signing this agreement, I agree to take full responsibility for the loan equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.
- b. I understand that I am responsible for the equipment at all times whether on the school's property or not.
- c. I agree to keep the equipment in good condition and to return it to the school/trust on demand in the same condition.
- d. I will not leave the equipment unsupervised in unsecured areas.
- e. I will take the following measures to protect the device:
  - i. Keep the device in a secure place when not in use
  - ii. Not leave the device in a car or on show at home
  - iii. Not eat or drink around the device
  - iv. Not lend the device or allow anyone to use the device unless required in the course of my work.
  - v. Not leave the equipment unsupervised in unsecured areas
  - vi. If the equipment is stolen, I will also immediately inform the police.
- f. If I do not follow the actions laid out in c-e then **I accept that am responsible for the reasonable costs requested by the school to repair or replace the equipment.** If the equipment is stolen, I will also immediately inform the police.

### 8. Unacceptable use

- a. I am aware that the school IT service providers monitor my activity on this equipment.
- b. I will not carry out any activity that constitutes 'unacceptable use'. This includes, but is not limited to the following:
  - Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Sharing confidential information about the trust/school, its pupils, or other members of the trust/school community
  - Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
  - Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- c. I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the trust's policies on staff discipline and code of conduct etc.

## 9. Personal use

I will not use this device for **personal use** and will not loan the equipment to any other person.

## 10. Data protection

I agree to take the following measures to keep the data on the device protected.

- a. Keep the equipment password-protected - strong passwords are at least 8 characters long, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- b. Make sure the equipment locks if left inactive for a period of time
- c. I will not share the equipment among family or friends
- d. Update antivirus and anti-spyware software as required
- e. Install the latest updates to operating systems, as prompted
- f. If I need help doing any of the above, I will contact AIT by use of a support ticket.

## 11. Return date

- a. I will return the device in its original condition to the school office/trust head office within 14 days of being requested to do so.
- b. I will return the equipment to the school/trust upon resignation, dismissal or if leave the employment of the school/trust for any other reason.

## 12. Consent

By signing this form, I confirm that I have read and agree to the rules and conditions set out above.

<b>Employee's full name:</b>	
<b>Employee's signature:</b>	
<b>Date:</b>	

## Part 2 - Record of loan

To be filled out by both the staff member signing out the equipment and the staff member receiving the equipment. **To be retained in school/head office (for trust staff).**

<b>Details of staff member in receipt of the equipment</b>	
Employee Name	
Role	
School/Trust	
<b>Loan details</b>	
Date of Issue	
<b>Equipment Details</b>	
Type	
Make	
Model	
Serial Number	
Replacement Value	
Equipment Condition	
<b>Accessory Details</b>	
Description	Quantity
<b>Equipment Return</b>	
Date Returned	
Equipment returned in original condition?	<b>Yes</b> <b>No</b>
<b>Comments if not in the original condition:</b>	