ICT Responsible Use Policy (ICT RUP)

This policy is also linked to the following school policies which can be found at http://www.bedmod.co.uk/the-school/general-information/school-policy-documents/ for staff and visitors (where applicable):

- A Simple Guide to the General Data Protection Regulation
- Code of Conduct Policy
- Concerns and Complaints Policy
- Disciplinary Policy
- Grievance Policy
- Harpur Trust General Data Protection Regulation (GDPR) Policy
- Harpur Trust Information Security
- Harpur Trust Social Media Policy
- Health, Safety and Fire Policy
- Online Safety Policy
- Staff Email and Internet Protocols
- Safeguarding and Child Protection Policy

Scope of this Policy

This policy applies to staff. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship) either connecting to the school hard wired network or wireless networks ('BMS', 'BMS-Secure', 'BYOD', 'HTO-Access' 'GUEST' or 'BMS-Chromebook').

The word 'device' means a privately owned or School-owned wireless and/or portable electronic piece of equipment that includes laptops, netbooks, Chromebooks, smart phones, mobile phone, wearable technology, tablets/iPads, slates or other applicable device.

This Responsible Use Policy is intended to ensure that:

- Staff will be responsible users and stay safe while using the Internet, School network and other communication technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and other users at risk.
- Users are protected from potential risk in the use of ICT in their everyday work.
- Clear guidance on how to minimise risks and how to deal with any infringements are provided.

The school will try to ensure that all members of the school community will have adequate access to ICT to enhance their work or learning opportunities for students (where applicable) and will, in return, expect all users to agree to be responsible users.

Introduction

The use of Information Technology at Bedford Modern School is viewed as an essential resource for all members of the school community and the school is constantly looking at ways to improve and develop ICT.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside of school.

The Internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and raise awareness of context to promote effective learning. All users should always have an entitlement to safe Internet access.

This policy is intended to address both school owned computer hardware in addition to the use of non-school owned electronic devices by students. These include all devices used to access the Internet and/or store school information as well as users' own data. This is commonly referred to as 'Bring Your Own Device' (BYOD). The school recognises that mobile technology offers valuable benefits to students from a teaching and learning perspective. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

This policy covers the use of all devices and the liability of the school for mobile devices used on school premises. The use of devices on school grounds is at the discretion of the school. Users can be granted the right to use their mobile devices if they adhere to this **ICT Responsible Use Policy (ICT RUP)** together with any associated polices and accept the agreement and guidelines set out herewith.

Responsible Use Policy Agreement

- Where appropriate all users should familiarise themselves and follow the guidance as outlined in the linked policies. All parts of this ICT Responsible Use Policy and associated policies should be understood fully prior to acceptance and any questions that arise should be directed to the e-Safety co-ordinator or the ICT Services and Innovations Manager.
- Staff should understand that they must use School ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. They should recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. Staff will, where possible and if appropriate, educate the young people in their care in the safe use of ICT and embed online safety in their work with young people.
- Whilst exciting and beneficial both in and beyond the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and must read and sign this ICT Responsible Use Policy prior to using their provided network login details.
- When users use their own personal devices in School, they will follow the rules set out in this agreement in addition to the separate **Online Safety Policy**, in the same way as if they were using School equipment. They will also follow any additional rules set by the School about such use and ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- Networked computers will gain access through the school's firewall, which is maintained by the ICT Services Department. However, no firewall is impenetrable so additional security products will be used in conjunction with the firewall. However, all School users are expected to maintain a level of 'personal responsibility' when using our system and any mobile technologies onsite and access via any illicit means to undesirable websites will be treated as a threat to our community and system integrity and users may be disciplined accordingly.
- Staff should be aware that compliance with this policy is mandatory.

School Internet and E-mail Systems

- Bedford Modern School will provide a filtered educational internet and email service which is monitored in school and by our provider to reduce the risk of access to inappropriate material. In order to protect users further the school will have the capability to decrypt all secure web (HTTPS) traffic user sessions on all computers connected to the school's wired and wireless network (via the installation of a digital certificate). Therefore, any user that connects their device to the schools 'BYOD', 'GUEST' or 'BMS-Chromebook' wireless networks are advised to install a digital certificate onto their personal device/s to avoid receiving errors whilst using the Internet.

  Bedford Modern School will however have a 'whitelist' detailing which websites to decrypt, so data is only decrypted where the safeguarding of users is necessary.

  For further information on SSL, please refer to **Appendix B**: *BRING YOUR OWN DEVICE (BYOD) Frequently Asked Questions (FAQ'S) sheet*, within this ICT Responsible Use Policy (ICT RUP).

- Staff must be aware that some services available on the Internet may be offensive. Whilst the School takes reasonable and necessary precautions, including filtering and other security measures, to help ensure a safe computing environment for users, the School cannot make an absolute guarantee that a user will not be able to access relatively inappropriate material, and the School cannot be held responsible for the voluntary actions of the users in this regard.

- The school provides internet (web site and application based) filtering for all users utilising School owned computing devices in addition to personally owned computing devices as long as the user connects to the internet via the School supplied wireless network and Internet Gateway. All internet access via the network is filtered, monitored and logged.

- Whilst students are not permitted to connect or 'tether' any school owned computer equipment through non-school controlled or managed wireless or network systems, such as personal 3G, 4G or 5G networks, 'Hotspots', Proxy or VPN bypass Systems, staff are permitted to do this as they will be protected by Web Filtering Software on their School provided laptops.

- The school will not be responsible for any content accessed by a user using their own devices through non-school controlled wireless or network systems, such as personal 3G, 4G or 5G networks, 'Hotspots', Proxy or VPN bypass Systems.

- The school accepts no responsibility for information or material contained on any website; other than its own.

- Bedford Modern School's e-mail and Internet facilities are primarily provided to its users for School related teaching and learning or business purposes only. Any use of the systems for personal or recreational purposes should be within the policies and rules set down by the school, as follows:

  - Personal use of the Internet must not interfere with a user's work commitments (or those of others). If it is discovered that personal usage has been excessive, disciplinary action may be taken and access to the facilities may be withdrawn without notice. The school reserves the right to undertake random checks of users' Internet and email usage.

  - Staff are not permitted to enter into any contract or subscription on the internet on behalf of the school, without specific permission to do so.

- E-mail should be treated in the same way as any other form of written communication. Users should not include anything in an e-mail which is not appropriate to be published generally. They should exercise care when copying or forwarding e-mails as this may disclose sensitive or confidential information to the wrong person and may breach data protection laws.
- Staff should be aware that e-mails are disclosable as evidence in court proceedings and, even if they are deleted, a copy may exist on a back-up system or other storage area.
- An email message which is abusive, discriminatory on ground of sex, marital or civil partnership status, age, race, disability, sexual orientation including being or becoming a transsexual person, pregnancy and maternity or religious belief (or otherwise contrary to our Equal Opportunities policy) or defamatory is not permitted.
- Statements criticising competitors, staff, students or parents and those stating problems with services, suppliers or customers should be avoided.
- Personal emails must not be accessed on any school equipment. Any school equipment should only be used in accordance with the **Online Safety Policy**. If staff wish to access a personal account during their time at work this must be done via their own device, and not on a school/Trust computer/tablet e.g. iPad, as doing so significantly increases the risk of infecting the school network with ransomware or other malware.
- Staff should also refer to guidance set out within the **Email and Internet Protocols Document and Staff Code of Conduct Policy.**

- Staff must not export any school or Harpur Trust related personal information onto any personal device. The issue of users exporting personal information onto their own computers/devices is that the device is not managed by the school and therefore could cause issues with regards to Data Protection if the user's personal device is compromised, lost or stolen.
- The School can monitor users' Internet, email and network activity; without consent in the following circumstances (in accordance with the Telecommunications [Lawful Business Practice] [Interception of Communications] Regulations 2000): to ensure compliance with regulatory practices; safeguarding purposes; to ensure standards of service are maintained; for any lawful purposes including the prevention and detection of crime, serious conduct or welfare concerns, extremism or the protection of others; to protect the communication system (including unauthorised use and risk of viruses).
- Care should be taken when opening files or e-mail attachments received via the Internet or web-based e-mail providers. If there is any doubt or concerns regarding the contents, then please delete the files. If you have any concerns, you should contact the ICT Services/Support Department as soon as possible.
- Information received from the Internet should not be uncompressed or executed unless the source is trusted. Under no circumstances should unsolicited data or files be opened, uncompressed or executed.
- Staff should take care when opening any hyperlinks in emails or any attachments to emails, unless the source is known and trusted. If they have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes) they should not open it.
- All devices being used to receive or send School e-mail must have virus protection software installed and be kept up-to-date.

- Anyone accessing emails via their personal devices must have that device password protected and must have the ability to delete data should the device be compromised.
- Bedford Modern School will not be responsible for any unauthorised financial obligations resulting from user's activities on the internet.
- Your school email address must not be used for any non-work or personal websites. Your school email address is issued to you by the school for school business only.

Set out below are examples of inappropriate use of the School's Internet and e-mail facilities, which are by no means exhaustive:

- Staff must not use any software that supports the illegal or legal download of materials using the school's Internet (including 'live' multiplayer games and file/data sharing software like Bittorrent, etc).
- The use of technology that would be considered an act of plagiarism is not permitted.
- Staff should not try (unless they have permission) to make large downloads or uploads that might consume internet capacity and prevent other users from being able to carry out their work.
- The use of any 'Proxy' or 'VPN' avoidance/bypass sites/software/systems used to gain access to restricted sites, i.e., social networking sites (during lesson time), gambling, pornography or any other form of unauthorised activity.
- The creation, downloading, storage, processing or transmission of any form of obscene, indecent or offensive material or pornography in any form (e.g. scenes of extreme violence or injury, scenes of sex or partial/entire male/female nudity, bad taste humour). This includes written, photographed, drawn or animated formats or any data capable of being resolved into such material.
- The unauthorised accessing, downloading or distribution of confidential information about other students, the school, its staff or their families.
- The accessing, downloading or distribution of copyright information and/or software including illegal downloading and copying of games, music, movies and other protected works, in breach of the Copyright, Designs and Patents Act 1988.
- The use of the e-mail system for the purpose of 'spamming' (e.g. large scale distribution of unsolicited e-mail to other users, both internally or externally, sending or copying of chain letters, jokes, gossip, movies or cartoons).
- To intercept or view an e-mail message or attachments that was originally destined for someone else.
- The use of another e-mail account other than your own to impersonate another person in a malicious context irrespective of how the logon details to that account were obtained.
- If users open inappropriate material this must be reported immediately to the school's e-safety co-ordinator who will address the matter in conjunction with the ICT Services/Support Department.
- Should users receive an e-mail that has been wrongly delivered to their e-mail address, they must notify the sender by re-directing the message to that person and then delete the original email.

School's Network

- All access to the network in school will be supervised and available only to those who possess a valid network username and password. Students should be reminded of the need for password security and must:
    - Use a strong password. Passwords should have the following characteristics:
        - A minimum length of 10 characters will be enforced.
        - Users must be able to change their passwords at any time.
        - Reuse of the 12 previous passwords must be prevented.
        - ***Users should be forced to change their password after a period of 360 days. A minimum password age 0 days will be set.***
        - *Repeated entry of invalid logon credentials must result in the account being locked.* ***This will be triggered after 5 consecutive invalid attempts.***
        - Passwords must be set to include characters from 3 of the following 4 categories:
            - Uppercase letters
            - Lower case letters
            - Base 10 digits (0 through to 9)
            - Non-alphanumeric characters (special characters)
    - Never share or disclose details of the school's network or technical information including login information with any other person, either directly or indirectly. No student should impersonate another user by using their login information.
    - Not write down or store a password where it is possible that someone may steal it.
    - Not use your school network password for any external websites and services that are not synced and managed by IT Support, that are work/school related and use your school email address. The password used must be a different password to the one you use on the network.

      Advice and guidance on how to set simple but strong passwords can be referred to in **Appendix A**, included within this ICT Responsible Use Policy (ICT RUP).
- The issue of a username and password is conditional upon acceptance and signature of this appropriate user agreement. We reserve the right to suspend or discontinue access to the network for activities which we consider inappropriate in an educational setting. All users' network and School IT access will cease upon them leaving Bedford Modern School.
- Personal devices must **NOT** be plugged into the school's local area wired network via an Ethernet cable or connected to the school 'BMS' network without approval from the ICT Services & Innovations Manager. Only personal wireless devices may be utilised, through the school's 'BYOD' (for students and staff), or 'HTO-Access' (for governors) wireless network. The school's wireless network is used only for access to the internet. No other School resources may be accessed directly, unless accessed through a secure portal.

- The school maintains a number of protective mechanisms to keep unauthorised, unfriendly and malicious users from accessing School resources. These systems are operated and maintained by the ICT Support/Services Department, and users may not bypass these systems by any means. Other than reporting suspected malfunction, normal School users should not have any concern for these systems, including:
    - Firewalls between school resources (including Servers/Services) and the Internet.
    - Intrusion Prevention Systems (IPS).
    - Web Application Firewalls that protect School hosted systems.
    - Web and application filters.
    - Email virus, malware and spam scanners/filters.
- Personal devices must not interfere with the normal operation of School owned devices and users should never attempt to use them in any way to act as a means/tool for circumnavigating the school's security systems.
- Bedford Modern School may monitor, with specialist software, user's network activity for safeguarding and welfare purposes and to reduce the risk of access to inappropriate material.
- Resourced networked printers are in use at the school and printing is controlled, therefore users should only print materials they require in order to minimise waste. Physical **vandalism** is prohibited. Examples of physical vandalism include, but are not limited to, the following examples: disconnecting wires on the back of the computer, tearing off labels and other attachments, carving or marking anything onto computer hardware.
- Electronic **vandalism** is prohibited. Examples of electronic vandalism include, but are not limited to, the following examples: opening/changing/deleting files, changing desktop patterns or sound.
- Licensing of software is for Bedford Modern School use only; and not the individual user (unless specifically instructed).
- Staff should not attempt to compromise the security of the school's network. Examples of this include, but are not limited to, unauthorised access (hacking) into School technical hardware, i.e. servers, network switches, printers, etc; therefore, adhering to the Computer Misuse Act 1990.
- No staff should log onto the e-mail, Internet or School network systems and knowingly or negligently leave the workstation unattended for use by another person. The school accepts no responsibility for loss of data or privacy that may occur as a result.
- Staff are not permitted to use any Human Interface Devices (HIDs) on school provided/owned computers for any malicious purposes, such as to inject keystrokes into a system, steal user credential data or to inject payloads such as malware or computer viruses onto school computers.

Data Encryption, Data Security and Data Storage

- Staff are permitted and encouraged to store or save their data onto the school's secure central server, shared Microsoft Office 365 area or, where available, within their School Microsoft Office 365 personal online account.

- Where possible portable storage devices such as USB data sticks will be encrypted before use with individual passwords. The school will enforce the encryption of USB portable storage devices when accessed on the school network. Users are encouraged however not to store any sensitive or personal data on any portable devices.
- Staff must take all sensible measures to protect information including but not limited to the use of authenticated access to their own device (i.e. requiring a PIN, pattern or password to be entered to unlock the device).
- Staff should also ensure their device auto-locks if inactive for a period of time. The school reserves the right to remotely wipe school email stored on a device in the event of loss or theft.
- Access to certain School or Trust Systems may be secured further by the use of a technology called Two-factor authentication (also known as 2FA or 2-Step Verification) that provides identification of users by means of the combination of two different components. Use of this technology will be enforced for Staff accessing Microsoft Office 365 (emails and OneDrive) and the School's Management Information System via remote links from places such as their home or outside the school. This offers greater account security by requiring Staff to authenticate their identity with more than one method. This means that, even if someone were to get hold of a primary password, they could not access the account unless they also had access to a mobile phone or another secondary means of authentication.
- If a handheld device cannot be encrypted it must not be used and will not be permitted by the school to store person identifiable data or School emails. Furthermore, it must not be connected to any of the school systems, whether by physical (e.g. USB) or wireless connection (e.g. Wi-Fi).

  The school aims to replace any devices which cannot be encrypted and which are capable of storing personal data where it is possible to do so.
- Most of the information accessed via a user's own device should not be private. If, however, information is accessed which is deemed to be private then this should be treated as such and not shared amongst the school community.

  In the event that information has been accessed which is considered private or protected, the incident must be reported to the School's ICT team as soon as possible. Any sensitive or personal data must be securely deleted when it is no longer required.
- Staff will not publish any documents containing personal data or critical information on externally accessible websites, unless remote (Internet) access to this data is configured to require user authentication.
- The school takes its compliance with the General Data Protection Regulation (GDPR) seriously and always aims to keep personal data secure. It takes suitable measures to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of or damage to personal data. All members of School Staff and Governors are required to undertake Data Protection training using the school's e-learning and compliance management platform. The training provided is designed to help Staff understand key areas of compliance and also to provide evidence that staff have read and understood relevant policies and documents.
- Regular monitoring checks will be undertaken to ensure compliance with the criteria set out above.

- All incidents resulting in a breach of these guidelines must be reported to the School's Data Protection Officer (Director of Operations).
- Staff will only transport, hold, disclose or share personal information about themselves or others, as outlined in the **Harpur Trust General Data Protection Regulation (GDPR)Policy** and **Harpur Trust Information Security Policy.**
- Staff will not be permitted to remove or copy sensitive or personal digital data from the school network unless the data storage device is encrypted and is transported securely for storage in a secure location.
- Paper based protected and restricted data must be held in lockable storage. Staff must make sure they have a valid purpose to have any data in print and if data has been printed off it needs to be securely disposed of once it is no longer required. Staff should think before they leave data unattended.
- Wherever possible staff should use School-based programs to access and store information they need and should always ensure the ongoing confidentiality and integrity of any administrative and/or teaching and learning Management Information System and/or services that they use. Staff should not export any sensitive or confidential student/parent/staff data into from any System and store this data on their home/public computer or device.
- Staff should understand that General Data Protection Regulation Policy requires that any staff or student data to which they have access, will be kept private and confidential, except when it is deemed necessary that they are required by law or by School/Trust policy to disclose such information to an appropriate authority. Therefore, Staff should not send personal data to anyone unless you are legally required to, have the person's permission or a valid reason to do so – if you are not sure, ask someone.
- Any user that sends email attachments containing private, personal or sensitive data must encrypt this via content encryption and it is the user's responsibility to ensure that this happens. The user will be provided with the necessary training to enable them to encrypt files.
- If Staff are planning to purchase or use any online IT systems or services that store or process student or parent personal data, they should in the first instance liaise with the ICT Services and Innovations Manager in order for a GDPR Data Audit and Data Protection Impact Assessment to be undertaken.
- The Data Controller (Director of Operations) in the school is responsible for ensuring that personal data stored on School systems regarding staff, students and parents is appropriately restricted and only accessible to designated individuals. Staff are strictly prohibited from storing student or parent data on their own personal devices. Staff are therefore expected to act responsibly if using their personal mobile device for School business. They must delete sensitive or commercial emails from their device once the task has been completed and also delete any attachments to emails e.g. data sets/spreadsheets once finished.
- Staff should also refer to guidance set out within the **Email and Internet Protocols Document, Staff Code of Conduct Policy** and **A Simple Guide to the General Data Protection Regulation.**

Appropriate use of Social Networking/Media Sites, Artificial Intelligence (AI) Platforms/Sites and Online Safety

- Social media is a fun part of everyday life, but it can carry risks. The following bullet points are intended to help staff avoid any pitfalls, while still making best use of social media for teaching/learning and research as well as social purposes.

'A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chatrooms, media posting sites, blogs and any other social space online. They include, but is not limited to, sites such as Facebook, LinkedIn, Twitter, YouTube, Instagram, TikTok.'

- Staff should familiarise themselves and follow the guidance as outlined in the **Harpur Trust Social Media Policy and Online Safety Policy.** .
- Staff must not use any social network site to attack, abuse or bully any School staff, other students or people. The privacy and the feelings of others should be respected at all times. Students may be required to remove internet postings which are deemed to constitute a breach of this policy.
- Staff must not include contact details or pictures, etc. of other students or members of staff without their prior permission.
- Staff are strongly advised to not use any social networking site or pages in any way that may compromise current or future employment at the school. Any content that staff post about themselves, or others could be brought to the attention of the school, future employers or professional bodies and may be detrimental to further study and/or future careers.
- Staff should never reveal confidential information about the school or its staff or students. This might include aspects of school policy or details of either internal or private discussions. Please consult your Line Manager if you are unclear about what might be confidential.
- Staff should take effective precautions when using social networking sites to ensure their own personal safety and to protect against identity theft.
- The use of emerging technologies must be used with caution and if it was used inappropriately it would be considered a breach of this policy.
- Staff must communicate with others in a professional manner, and not use aggressive or inappropriate language appreciating that others may have different opinions. Staff will only communicate with students and parents/carers using official School systems.
- Approved staff with administrative rights to upload images that Marketing are aware of are permitted to use their own device to take and/or publish images of others but must delete them from their device immediately after uploading them. Staff will not use their personal equipment to record these images, unless permission has been granted to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- Staff must only use chat and social networking sites in School in accordance with the School's policies. (Staff should refer to the separate **Harpur Trust Social Media Policy**).
- Staff must not engage in any on-line activity that may compromise their professional responsibilities.

The use of personal devices in School

- The user takes full responsibility for his or her device. The school is not responsible for the security (including loss, damage or theft) of any device that is not defined as the property of the school.

School insurance cover will therefore not be applicable or valid. The school would therefore encourage all staff, volunteers and governors to extend their home insurance policy under the personal possessions section or alternatively cover electronic devices by a separate policy.

Insurance is, of course, a personal decision, but if staff, volunteers, governors and visitors/guests choose not to insure such items, please be aware that the school's insurance policy does **NOT** cover users' personal possessions.

If a device is stolen from the school grounds the school will investigate the theft. Wilful damage to devices will also be investigated by the school. Reception must be notified immediately of any incidents, and these will be logged.

- The user is responsible for the proper care of their personal device, including any costs of repair, replacement or any modifications needed to use the device at School.
- Bedford Modern School takes no responsibility for supporting students, staff, volunteers, governors and visitors/guests own devices; nor has the school a responsibility for conducting annual Portable Appliance Testing (PAT) on personally owned devices. However, basic assistance may be provided to the users by the School's ICT technical support team in establishing an initial connection to the 'BYOD', 'BMS-Chromebook', HTO-Access or 'GUEST' wireless network or the installation of the digital SSL certificate.
- Bedford Modern School reserves the right to inspect a user's personal device if there is reason to believe that they have violated School policies, administrative procedures, School rules or have engaged in other unacceptable behaviour while using their personal device on School grounds.
- Violations of any School policies, administrative procedures or School rules involving a student's or staff member's personally owned device may result in the withdrawal of permission to access the school network for individuals or groups at any time and/or may also be subject to disciplinary action.
- It is compulsory that any personal device being used to receive or send School e-mail or access to the internet has virus protection software installed and kept up to date. The installation and updating of the software will be the user's responsibility. It is the device owner's responsibility to keep any software and security settings on their own devices up-to-date.
- If in any doubt users should seek clarification and permission from the School's ICT team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school wireless system.
- The school is not to be held responsible for the content of any 'Apps', updates or other software applications that may be downloaded onto the user's own device whilst using the School's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability for any consequential loss of data or damage to the owner's device.

  Access to any educational software or applications will be provided to staff via a secure application portal.
- Personal devices shall be charged prior to bringing it to school and shall be capable of running off its own battery while at School.
- Users may not use their devices to record, transmit or post photos or video of a person or persons on site unless directed to do so and under strict supervision.

Neither can any images or video recorded at School be transmitted or posted at any time without the express permission of the school.

- Access to the internet through the school's wireless network is in a trial state. Changes may have to be made as we evaluate how it is working and it is important to understand that Bedford Modern School has the right to make any necessary changes to how the wireless access works for the best interest and security of students, staff, volunteers, governors, or visitor/guest users.
- For further information, please refer to **Appendix B**: *BRING YOUR OWN DEVICE (BYOD) Frequently Asked Questions (FAQ'S) sheet*, included within this ICT Acceptable Use Policy (ICT RUP).

Users working from home

All users are still responsible for keeping work or School information safe when accessing it at home.

These tips can help to minimise the chances of any cyber security incident transferring from home devices to the school network or vice versa.

- Use up-to-date anti-virus software on your own devices.
- Download all software updates as soon as they are available.
- Ensure **all** your devices have passcodes. (Even if you only use your laptop for work/School purposes, for example, this may be synched to your phone or tablet).
- Change any default passwords on devices or software – including your home Wi Fi.
- Switch on two-factor authentication (2FA) for sensitive accounts.
- When accessing School or Harpur Trust related personal information at home you must use a School provided device.

Acceptance of ICT RUP

As a member of staff, I have read and understand the Responsible Use Policy (together with any linked policies) and agree to use the School/Trust ICT systems (both in and out of School) and my own devices (in School and when carrying out communications related to the school) set out within these guidelines.

Signed _____

Date _____

D Donoghue
E-Safety Co-ordinator

Mr A Felice
ICT Services and Innovations Manager

Mr M Price
Deputy Head (Academic and Innovation)

February 2024
Review Date February 2025

Appendix A

Password Security

Passwords are your protection against your personal, private and school information being compromised and used without your consent. Being hacked can lead to your personal details and those of your friends and colleagues being compromised too. The best defence is herd immunity - everyone keeps everyone else secure.

If you use the same PIN number or password for multiple systems then your details can be re-used and access can be gained across different systems. If someone gains access to your email and then resets your password by sending a link to your email then they have access to that system as well. In this way your bank, your social media accounts, your personal and school records can all be accessed.

Hackers will routinely try a list of passwords containing many lists of commonly used passwords in multiple languages, including variations like P@55W0Rd or similar. They can try hundreds of thousands of these a minute with automated systems designed to crack passwords. A short password (7 characters or less) can be hacked in a matter of hours even if it is completely random.

Guidance on password security includes:

- A minimum length of 12 characters will be enforced.
- Users must be able to change their passwords at any time.
- Reuse of the 12 previous passwords must be prevented.
- Users should be forced to change their password after a period of 90 days.
- Repeated entry of invalid logon credentials must result in the account being locked. This will be triggered after 10 consecutive invalid attempts.
- Passwords must be set to include characters from 3 of the following 4 categories:
  - Uppercase letters
  - Lower case letters
  - Base 10 digits (0 through to 9)
  - Non-alphanumeric characters (special characters)

Click the link below for a list of the most commonly used passwords. Please also avoid using common passwords, such as a pet's name
http://www.passwordrandom.com/most-popular-passwords

So what can you do?

Making a better password involves:

- It must be hard to deduce or guess
- It must be easy to remember
- It must be easy to enter (on PC, Tablet, Phone)

What if you could have an easy to remember password that is difficult to guess or predict?

Better Passwords

A better password is twelve or more characters long and contains numbers, upper- and lower-case characters and punctuation.

You might think this would be difficult to remember but it needn't be:

- Purple.Elephant.H2O
- Zero-Emit-Radio

- Turbo-Fruitcake-365
- Animated.bingo.wins

These are examples of good passwords that are extremely hard to guess but relatively easy to remember and easy to type into a mobile device. With three easy to remember words it is possible to come up with a unique address for every location on the planet, as demonstrated here: http://what3words.com/ (please do not use your address location for a password as that too would be like using your postcode and is easy to guess for anyone who can look you up).

So, using three simple words and a separating character you can easily generate a memorable, easy to use, secure password. You can then have separate passwords for different services you are using so that you don't, for instance, use the same password for the school MIS as you do for email.

If you have any concerns about network security or would like help changing your password, then please feel free to come to IT Support and we will assist.

Many thanks for your help in keeping the School and Trust secure.

Appendix B

Bring Your Own Device (BYOD)

Frequently Asked Questions (FAQ'S)

Q: Is the Bring Your Own Device (BYOD) scheme open to all staff?

A: The Bring Your Own Device (BYOD) initiative is currently open to all staff but may be subject to change.

Q: What personal ICT Devices are permitted for use in School by staff?

A: Staff can use either a laptop, tablet device, smart phone, Chromebook or any other compatible device that supports the 802.1x wireless standard.

Q: What personal ICT Devices are <u>not</u> permitted for use in School?

A: Computer desktop computers are not permitted to be used as part of the BYOD programme. Any device that does not support the 802.1x wireless standard is not compatible for use on the wireless network.

Q: Can staff physically plug their devices into the School Network using a network data cable?

A: Staff should **not** plug their device, directly into the school network using a network cable. Access to the network can only be permitted via the 'BYOD' wireless network.

Q: Does the School provide any ICT technical support for any issues that arise with the student's personal devices?

A: Resources will be provided to help staff connect their device to the school network. However, the School will not provide technical support.

Q: Are personal devices insured under the school's insurance policy?

A: No. Members of staff should take full responsibility for their device and keep it with them at all times or locked away. The school is not responsible for the security (Including loss, damage or theft) of any device that is not defined as the property of the school.

School insurance cover will therefore not be applicable or valid. The school would therefore encourage all members of staff to extend their home insurance policy under the personal possessions section or alternatively cover electronic devices by a separate policy. Insurance is, of course, a personal decision, but if staff choose not to insure such items, please be aware that the school's insurance policy does **NOT** cover staff' personal possessions.

If a device is stolen from the school grounds the school will investigate the theft. Wilful damage to devices will also be investigated by the school. Reception must be notified immediately of any incidents, and these will be logged.

Q: How can staff charge their ICT devices at school?

A: Devices should be charged at home. All electrical devices used in school need to be Portable Appliance Tested (PAT) so, for Health and Safety reasons, personal devices cannot be charged in School.

Q: Can staff use their device as a personal Wi-Fi Hotspot or broadcast their own wireless network to allow others to access the internet?

A: Staff are not permitted to use their device to broadcast their own SSID or use it as a 'Hotspot' so that it can allow others to access the internet by by-passing the school's wireless network whilst in School.

The school will not be responsible for any content accessed by a user using their own devices through non-School controlled wireless systems such as personal 3G, 4G and 5G networks, 'Hotspots', Proxy or VPN bypass Systems.

Bedford Modern School cannot permit access to non-filtered services for safeguarding reasons, and this includes all wireless services. Any student enabling such a network would be committing a gross breach of trust that could result in them no longer being able to use a personal ICT device in School. Additional sanctions for breaching School rules could also apply.

Q: Why are members of staff filtered and monitored on their own device? Shouldn't they be able to see what they want to on their own device?

A: The School is providing users with a service, whilst being committed to making sure the network is safe and secure as possible. This is also part of our wider duty of care. Any personal device using the school's wireless network is filtered, monitored and secured according to policy. Please note, the 'BYOD' wireless network is there to help support teaching and learning and not as a recreational tool. The school will not be responsible for any content accessed by a user using their own devices through non-School controlled wireless systems such as personal 3G, 4G and/or 5G networks, 'Hotspots', Proxy or VPN bypass/avoidance Systems.

Q: Can staff access any School specific teaching and learning software including their school network data files from their personal device?

A: Staff can access the Virtual Learning Environment in addition to a number of other Teaching & Learning Resources and Online Systems from a Secure Staff Portal. – Accessible via the Staff section of the School Website.

Staff can also login with their normal School network username and password and use Office 365 online – accessible via the Staff Portal

Office 365 offers the following benefits for users:

- Accessible from any computer with an Internet connection and also works across a range of mobile devices.
- Ability to create and store up to 1TB of data files into your OneDrive Data area using the Microsoft online apps for Word, Excel, PowerPoint and OneNote (no software installation necessary).
- Office 365 ProPlus. This is the option to install the full version of Microsoft Office on up to 5 devices (PCs or Apple Mac's); and Office Mobile on up to 5 mobile devices completely free of charge. This option will be available to all current Bedford Modern School students whilst they are registered with the School.

Q: Why are members of staff advised to download and install an SSL certificate onto their personal devices?

A: Protecting staff and other users from inappropriate or illegal material is a priority at Bedford Modern School and always will be. Therefore, in order to maintain our high standard of filtering and monitoring for users, the School will also have the capability to decrypt all secure web (HTTPS) traffic user sessions on all computers connected to the School's 'BYOD' or 'BMS-Chromebook' wireless network. Users are therefore advised to install a digital certificate onto their personal device/s to avoid receiving errors whilst using the Internet.

Bedford Modern School will however have a 'whitelist' detailing which websites to decrypt, so data is only decrypted where the safeguarding of users is necessary. For example, even though this technology has the capabilities to decrypt online banking websites, we will leave banking websites from the list of websites that we will decrypt.

Technical explanation

The reason that installation of the certificate is required is that over recent months, changes have been made by Yahoo, Google and other websites in the way it retrieves search results. It now diverts users to their HTTPS site, rather than the HTTP site that it previously used. The effect of this change compromised online safety as this disabled

some of the safety features available. Therefore, enabling HTTPS inspection (Using a technology called 'Man in the Middle') for users provides for the capability to decrypt the HTTPS session by encrypting transmitted data making it more difficult for snoopers to see personal confidential information. However, this means that any omission of a SSL certificate from the user's device results in the web filtering not being able to check Internet activity for inappropriate material which raises the risk that students could access inappropriate materials. Man in the Middle technology will decrypt traffic from sites on the whitelist (see above) enabling the usual e-Safety checks to continue safeguarding our users.

Q: Why are staff receiving certificate errors when browsing the Internet using their personal device?

A: The likely cause is because staff have not yet installed the digital SSL certificate onto their personal device.

Q: How do users download and install/import the digital SSL certificate for use on their personal device?

A: Once you have connected to the 'BYOD' wireless network, enter the following URL into your web browser: https://switchshop.info/bedford_modern
Or scan this QR code with a QR scanner application:

You will then be presented with some specific instructions on how to Download and Install/Import the certificate onto your personal device. As each Operating System and web browser have different methods to import the digital certificate, the Website will intelligently provide guidance based on the type of device that you are using.