POLICY FOR	**ACCEPTABLE USAGE FOR ICT, TELECOMMUNICATIONS, INTERNET & EMAIL**
PERSON RESPONSIBLE	**ICT NETWORK MANAGER**
REVIEW DATE	**Nov 2024**
NEXT REVIEW DATE	**Nov 2026**
APPROVED BY	**HEADTEACHER**
APPROVAL DATE	

Scope

This policy covers The Malling School.

Context

The term "User" in the context of this document refers to any member of staff or individual from another organisation that has an account allocated for their use on the network of The Malling School.

The term "School Network" refers to all services offered and hosted by The Malling School, this includes any external services that hold school data including, but not limited to Microsoft 365.

The Malling School Acceptable Usage Policy still applies when accessing systems from home or any remote location. This also applies to using any laptop, mobile phone or portable computer device owned by the school at all times, even when not connected to the school network.

Aims

We recognise that users at the Malling School have the necessity to use computers, the internet & e-mail. However, we also recognise that these facilities carry with them risks and liabilities. It is therefore essential that users at The Malling School accept and adhere to the guidelines in this document, in addition to any potential liabilities involved in using computers, the internet & e-mail.

Any breaches of this policy may result in disciplinary action in line with the appropriate disciplinary procedures. This policy also relates to the appropriate Code of Professional Conduct. All misuse of ICT systems may be treated as misconduct and in some cases may be treated as gross misconduct.

Acceptable Use

The Malling School ICT resources are provided primarily for academic and operational purposes to support teaching and learning, research, enterprise and the other work of the school. Facilities are also provided to pupils to enhance their wider experience at The Malling School.

Whilst the principles of academic freedom will be fully respected, facilities must only be used responsibly, in accordance with the law and not to bring the school into disrepute.

Staff at The Malling School can access school facilities using either school-provided equipment or their own personal devices, but this policy is applicable regardless of the ownership of the device used. However, personal devices must have up-to-date anti-virus software (if applicable), system patches, and must be kept secure. When using personal devices (laptops), staff must connect to the public Wi-Fi on a separate network for security, at their own risk. Staff may also connect their personal mobile devices to the BYOD network. If taking school equipment offsite, staff must comply with GDPR requirements and return the equipment at the end of their employment.

Students at The Malling School can access school facilities using school-provided equipment on-site or their own devices outside of school. This policy applies regardless of device ownership. Personal use of school facilities is not allowed. Students are not permitted to take school equipment home without permission from the headteacher or the ICT department.

Sixth form students may use their own device that has been subsidised by the school to meet our school requirements. These subsidised laptops are the responsibility of the students as they would own the device. Whilst the student is at the school, TMS will support warranty claims but will not assist with accidental damage claims. Personal use of school facilities is not allowed. The Malling School allows sixth form students to connect one additional personal device to the BYOD network. Students are not permitted to take school equipment home without permission from the headteacher or ICT department.

School e-mail addresses and associated systems must be used for all official school business, to facilitate auditability and institutional record keeping.

When using the school's ICT facilities, users remain subject to all relevant laws and policies, and, when accessing services from another legal jurisdiction, users must abide by all relevant local laws, as well as those applicable to the location of the service. Following the requirements of this policy, and other school policies and procedures users must ensure compliance with the law. However, if a user has any concerns about whether planned actions may be regarded as unlawful, they should contact the ICT Department for further advice.

Users must adhere to any licence conditions when using software procured by the school.

Further details of what constitutes acceptable and unacceptable use is provided in the subsequent sections of this policy.

Securing Login Credentials

All users must take reasonable precautions to safeguard their username, password and any other ICT credentials issued to them. When users first receive their password, you will be prompted to change your password to help prevent unauthorised access to their account. User passwords' must adhere to Microsoft complexity password policy. Users must not allow anyone else to use their ICT credentials. No one has the authority to ask users for their password, and passwords must not be disclosed to anyone, including the ICT Services department.

Password Guidance

To be able to create a strong password, users should be aware of the criteria required to create one. These criteria include the following:

- A strong password must be at least 8 characters long.
- It must not contain any personal information, specifically a user's real name, username, or company name.
- It must be unique from previously used passwords.
- It must contain at least one upper and lower case character, at least one number and recommends a special character.

Users must not attempt to obtain or use anyone else's credentials; and users will be held responsible for all activities undertaken using their ICT credentials. Users must not impersonate someone else or otherwise disguise their identity when using the ICT facilities.

General Computer Usage

1. Use of computers, telephones, the internet and e-mail is primarily for work related purposes.

2. The Malling School reserve the right to monitor and inspect all aspects of its telephony and computer systems.

3. The Malling School have the right to intercept or record any communications made by clients using our school network, including, but not restricted to, using telephone, internet & e-mail. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice/Interception of Communications) Regulations, users are hereby required to expressly consent to the school doing so.

4. Computers, telephones and e-mail accounts are the property of The Malling School and are intended for work purposes. Therefore, users must have no expectation of privacy regarding computers, telephones, e-mail and the internet, whether it be of a business or personal nature.

5. It is an inappropriate use of ICT systems for users to access or download material that can be considered to be obscene, defamatory or offensive to people who have protected characteristics, in accordance with the Equality Act 2010. Such material can also be contained in jokes sent by e-mail. If users receive material with content of this nature, the material must be reported. The Malling School reserves the right to use the content of any employee e-mail in any relevant disciplinary processes.

6. Any deliberate attempt by staff, learnings, visitors or volunteers to gain unauthorised access to facilities or system services via the school's network is prohibited. This includes attempts to

bypass web filtering, accounting and any login systems. This also includes any attempts to bypass any web filtering products to access websites which are prohibited by this policy.

7. Users must not transmit unsolicited commercial or advertising material via the school's network unless this is part of an official campaign authorised by The Malling School.

8. No software licensed to The Malling School shall be copied to a portable storage device or taken off site without the permission of the ICT Network Manager. Software owned by The Malling School must not be copied without specific instruction and must only be copied when appropriately licensed, or for backup purposes. The unauthorised or illegal copying of software may result in legal consequences and/or disciplinary procedures.

9. No software or hardware shall be installed on the school systems by any persons at any time without permission from ICT Services department.

10. Users must not deliberately waste staff efforts or networked resources, corrupt or damage another user's data, violate the privacy of others, disrupt the work of others or use the school's networks in a way that disrupts service to other users. It is recommended that all users carry out housekeeping tasks with regards to their network storage and mailboxes to remove any unnecessary overhead from the network.

11. PCs must not be left unattended whilst logged into the network, this creates a possibility of unauthorised access to the school's systems. PCs must be locked by using 'Windows key' and 'L' to ensure this does not happen. The school's accounts are issued on an individual basis so that usage of the systems can be held accountable to a single user. Allowing others to use your network accounts is strictly prohibited. Any actions done under an account are accountable to the owner of that account, and may result in disciplinary procedures that are appropriate to those actions.

12. Each user is responsible for the safeguarding of their passwords. For security reasons, individual passwords must never be printed, stored online or given to other persons. User password rights do not imply that the user has complete privacy. Do not use obvious words or phrases and try to pick 'hard to guess' random passwords.

13. If a user has the ability to connect to other computer systems through the network, that does not mean that the user can make use of those systems, unless authorised to do so. Files belonging to other users must not be altered or copied, unless permission has been obtained by the creator of the file.

14. Any sharing of personal data to third parties including full names or email addresses must comply with GDPR legislation. This includes paid or free trials where personal data is shared outside the organisation, and therefore any such sharing of data must be approved by the ICT department.

15. Staff may take their personally created files and documents when their employment ends at The Malling School providing they adhere to GDPR requirements and do not take any copies of personal information.

16. If users are using non-school equipment, they must use online cloud services for work and refrain from storing personal data on external or personal devices. To comply with GDPR policies and guidelines, all files and documents must be stored exclusively on school-approved platforms such as Microsoft 365.

17. Staff who use personal devices to access school data or applications such as Bromcom must have a pin number or biometrics enabled.

18. External storage devices are prohibited and will not function on the school network.

E-Mail Usage

1. E-mail is a legal means of communication and therefore subject to the Malicious Communications Act 1988 and the Communications Act 2003.

2. Users must not make derogatory remarks about employees, students, competitors or any other persons. Any written derogatory remarks may constitute libel.

3. E-mail must be drafted with care; e-mail is still a permanent form of written communication and can be recovered even when it has been deleted from your computer.

4. To ensure e-mail communication is effective and efficient, do not send trivial e-mails or copy in users unnecessarily.

5. Users may use e-mail confirmation and receipt of important messages. This is not always possible and may depend on the system receiving the message. If in doubt, confirm delivery/receipt of e-mail by telephone.

6. By sending e-mail on the school's system, the user explicitly consents to processing of any personal data contained in that message. If users do not agree with the school processing such data, another means of communication must be agreed by the ICT Network Manager.

7. Subscriptions must not be made to any list servers or discussion groups that transmit material that does not comply with the objectives of the school. This includes using a school e-mail address as a login name for third party sites.

8. The school's e-mail system is for communication purposes and not for data storage. Any e- mail attachment deemed important should be copied to the user's home directory or approved cloud-based platform.

9. Use of the school's e-mail is monitored, via random system checks and authorised investigations. Email algorithms are implemented for trends and security protection.

10. E-mail must be considered an unsecured medium when transmitting data. Sensitive and personal data must be transmitted by other means.

11. E-mail must not be automatically forwarded to third party accounts outside of the school e.g. Google, Yahoo etc. E-mails often contain personal or sensitive information which sharing would result in a breach of GDPR legislation.

12. Further guidance for staff on email protocol can be found in the staff handbook.

13. Any emails sent in error to the wrong recipient must be reported as a GDPR breach if the email contains any personal data that is not accessible to the recipient.

14. Emails that contain highly sensitive personal data must be encrypted before transmitting, using a strict password. The password used to secure the data must not be included in the original email. Its recommended to send this password separately or via a telephone call exchange.

15. Staff use email as a communication tool, it's important to check these regularly at an appropriate time.

Internet Usage

1. Limited private use of the internet is permitted but must not interfere with work and be confined to an employee's own time. The Malling School actively monitor internet use for content, and the amount it is used by individuals. Excessive private use of the internet may lead to disciplinary action, and in some cases will be treated as gross misconduct. If any material is viewed in error that does not meet our Acceptable Usage policy, a member of the ICT Services department must be informed. Failure to do this may result in later disciplinary action.

2. Any sites accessed must comply with the restrictions set out in this document.

3. Copyright applies to all text, pictures, video, and sound, including those received by e-mail or the internet. Music and video files such as MP3s and MPEG4s which are not free to distribute must not be downloaded or stored on any part of the school's network.

4. All internet usage at The Malling School is constantly monitored, via random system checks and authorised investigations. All visited web sites are clearly logged as well as times they were accessed.

5. The internet must be considered an unsecured medium when transmitting data. Any transactions that originate from The Malling School are carried out entirely at the user's risk. The Malling School is not responsible for any on-line fraud that may occur from personal use; or the loss, damage or misuse of data.

6. Staff must not set up any website or social networking site which has references to The Malling School without prior permission. References may include links, citations or images referring to The Malling School from a user's personal web space. Clearance for such sites must come from ICT Services, who will seek approval from the headteacher.

7. Any personal or social networking website of an individual user officially connected with The Malling School in the public domain must be conducted in a professional manner.

8. Any personal or social networking website of an individual user officially connected with The Malling School in the public domain must be conducted in a professional manner.

9. Staff and students are prohibited from installing VPNs or using similar software to circumvent the school's filtering system. Only the ICT department may install an approved VPN if necessary.

Bring your own device (BYOD)

Individuals using BYOD must take responsibility for their own device and its usage. They must:

- Connect laptops to the public WIFI, not the TMS WIFI network.
- Mobile phones can be connected to the BYOD network (staff and sixth form only).
- No Linux-based devices are allowed (Ubuntu etc…)
- Familiarise themselves with their device and its security features to ensure the safety of TMS information and their own information.
- Activate relevant security features.
- Regularly patch and upgrade the device.
- Ensure the device is not used in violation of the ICT Acceptable Use Policy.

TMS ICT staff will assist where possible, but TMS does not support devices it does not provide. Staff using BYOD must:

- Take reasonable steps to prevent theft and data loss.
- Keep information confidential where appropriate.
- Maintain data integrity.
- Be responsible for any software downloaded onto their device.

Staff using BYOD must also:

- Set up complex passwords, passcodes, passkeys or biometric equivalents.
- Encrypt documents or devices as necessary.
- Avoid storing sensitive, personal, confidential or commercially valuable information on personal devices.
- Use TMS services for secure access (Microsoft 365)
- Delete TMS information from personal devices as soon as it is no longer required, including information in emails.
- Copy relevant information back to TMS systems and manage data integrity issues.
- Report any device loss containing TMS data (including emails) to the ICT Helpdesk.
- Be aware of Data Protection issues and handle personal data appropriately.
- Report any security breaches immediately to the ICT Helpdesk, with the Data Protection Officer informed if personal data is involved.
- Ensure no TMS information is left on any personal device indefinitely, especially if the device is disposed of, sold, or transferred to a third party.

TMS will not monitor the content of user owned devices, but reserves the right to monitor any traffic over the school system to prevent threats to the school network systems. TMS also reserves the right to:

- Prevent access to a particular device from either the wired or wireless networks, or both.
- Prevent access to a particular system.
- Take all necessary and appropriate steps to retrieve information owned by TMS.

The TMS ICT department will not provide support for personal BYOD devices.

Data Protection and BYOD

TMS must process 'personal data', which includes information about identifiable living individuals, in accordance with the Data Protection Act 2018. Sensitive personal data encompasses information related to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (both mental and physical) and details of criminal offenses. This type of data requires a higher level of protection at all times.

Following the Information Commissioner's Office guidance on BYOD (Bring Your Own Device), TMS acknowledges the inherent risks of using personal devices for handling personal data. Therefore, staff must adhere to the guidelines provided in this document when using BYOD to process personal data.

A breach of the Data Protection Act can result in TMS being fined. Any staff member found to have deliberately violated the Act may face disciplinary actions, withdrawal of access to TMS facilities, or even criminal prosecution.

Social Networking

Social networking sites encourage individuals to post personal and sometimes intimate information which previously would have been considered private. Anyone posting information through this media, must accept that this information could become public knowledge. At this point, whilst the activity may have taken place outside of work, it is no longer reasonable to assume that it is personal and private and nothing to do with third parties such as employers and authorities. Pupils may be naïve in viewing this information and may, should they see staff role models in a different light, act differently or inappropriately. If activities are shown to have brought The Malling School into disrepute, a member of staff would be in breach of the Code of Professional Conduct and disciplinary action may be taken. Other activities or information could compromise staff professional relationships with pupils and colleagues. This applies to the use of social networking sites both inside and outside of the organisation.

1. Staff must not interact with pupils via social networking sites. This includes adding a pupil as a 'friend'. Any electronic communication to students and colleagues must be via a member of staff's school e-mail address.

2. Staff must not set up groups or social networking sites which represent The Malling School without permission from the headteacher.

3. When registering on social networking sites, staff must use a private e-mail account, rather than their school account.

4. Staff are strongly advised to consider their privacy settings on social networking sites. These must be regularly checked for compliance due to updating of security measures.

5. Privacy settings can change from time to time by providers. Any individual's social networking sites in the public domain, rather than private to friends only, must be in line with the Code of Professional Conduct.

6. Where specific use of the curriculum may require access to social networking sites for technical and programming courses, the guidelines within the AUP still apply.

7. All staff must also be aware that social networking sites can be used for cyber bullying. We have

a duty of care to our staff and pupils and will take appropriate action in accordance with our policies and procedures for the elimination of harassment and bullying, should we be aware that this is occurring. In addition, it is the responsibility of all staff to take appropriate action in accordance with these policies.

Cloud Services

- Cloud services are provided to allow staff and students to access learning materials and live lessons.
- Cloud services are provided in order to access data on personal devices off site.
- Data in cloud services should not be transferred to personal devices (GDPR).
- Cloud services must not be used on a public computer i.e. libraries, cafes etc.

Remote Learning, Online Lessons and Video Meetings

We recognise that using remote learning, including teaching through live streaming is different to teaching in the classroom. Teachers should ensure confidentiality when engaging in online lesson delivery and try to find a quiet or private space. When broadcasting a lesson or making a recording, teachers should be in a neutral area and ensure nothing personal or inappropriate can be seen or heard in the background. We recommend that web camera background is set to blur.

- Remote learning and video calls/meetings will only take place through approved platforms: Microsoft TEAMS, ZOOM and Parents Evening System.
- Staff will only use approved, professional school-managed accounts to engage with learners.
- Online contact with learners will not take place outside of operating times defined by the school.
- Staff will only record lessons or meetings using school equipment for educational use only.
- Where online lessons/meetings are required to be recorded, all participants must be informed and recording procedures must adhere to the schools Data Protection Policy requirements.
- All participants of online lessons/meetings are expected to behave in line with existing school policies and expectations.

Identification (ID Badges)

- ID badges must be worn on site at all times
- ID badges must not be borrowed or passed to another person
- ID badges must be returned to a member of the Human
- Any lost badges must be reported to HR or ICT for an immediate replacement

Printing

- Printing on school premises must be used for educational purposes only
- Staff will be issued with a printing code for secure printing, data logging and financial budgeting.

External Hosted Services

The school may use external companies to provide extra services to staff/student/parents. These could include:
Learning materials
Bromcom (MIS)
Microsoft 365 Education
Parents Evening Systems
Reporting Systems
Communications systems
Payment Systems

Appendix One: Acceptable Use Policy Acknowledgement - Staff

Signed in confirmation of policy compliance prior to system access being granted.

Please complete the following in BLOCK CAPITALS, sign and return to the ICT Network Manager or issuing member of staff

Full Name:

_____

Teacher or Support Staff

_____

Signature:

_____

Date:

_____

Access granted by: **Date:**

_____ _____

Appendix Two: Acceptable Use Policy Acknowledgement – Visitor/Volunteer

For visitors who require temporary access The Malling School ICT Networks.

The Malling School - Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are over the age of 18, you have read and understood, and agree to be bound by this agreement.

This wireless network is powered by Ruckus.

For those using WIFI provided by The Malling School.
As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools' boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.
This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. The school provides Wi-Fi for the school community and allows access for educational use and other business relating to the school. The Wi-Fi network is protected by a network password to prevent automatic connections to devices looking for open networks. Once connected users are required to enter a voucher code valid for a set amount of time to access the internet, codes supplied are unique to each individual in order to monitor their internet activity. Internet traffic is filtered in line with our policy for staff; this may mean that some website/services are unavailable.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within school premises that is not the property of the school.

3. The use of ICT devices falls under Information Systems: Acceptable Use Policy which all pupils/staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the schools' service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school's wireless is secure to industry standard WPA2-PSK (AES) but we cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.

12. My use of the school's Wi-Fi will be safe and responsible and will always be in accordance with the Information Systems: Acceptable Use Policy and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

16. No school or personal data will be removed from our network without permission and any data removed must be encrypted to meet GDPR legislation.

Kent Support and Guidance for Educational Settings

Designated Safeguarding Lead
Contact: Mr Chris Dmytruk
Email: chris.dmytruk@themallingschool.kent.sch.uk
Tel: 01732 840995
Mobile: 07842310034

Guidance for Educational Settings:

- https://www.kelsi.org.uk/child-protection-and-safeguarding
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links

Kent Online Safety Blog: www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCB: www.kscb.org.uk

Kent Police: www.kent.police.uk In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101.

National Links and Resources for Educational Settings:
CEOP: www.thinkuknow.co.uk www.ceop.police.uk
Childnet: www.childnet.com
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers:
Action Fraud: www.actionfraud.police.uk
CEOP: www.thinkuknow.co.uk www.ceop.police.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk