RICKMANSWORTH SCHOOL

Acceptable Use of ICT Policy

Version:	7
Version Author:	Rob Witcher / Jamie Taylor
Version Ratified By:	Full Governing Body
Date Version Ratified:	January 2021
Governor's Lead:	Qasim Latif
SLT's Lead	Emma Gritten
Date this version issued:	January 2021
Last Review Date:	March 2019
Next Review Date:	December 2023
Target Audience:	Governors, Staff, Students
To Be Published on The Website	Yes

Table of Contents

OVERVIEW

Purpose

ICT is an integral part of the way our school works and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents, governors, contractors, volunteers and visitors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use.
- This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Review Process

This policy will be reviewed every three years, on the introduction of new or amended relevant legislation, or if sufficient changes are made to the IT systems that would make this policy inaccurate.

Applying the policy

Staff and Students must sign the relevant appendix to confirm that they have read and understood the Acceptable Use of ICT Policy. The policies have been attached at Appendix A and B. Year 7 students will be sent the Acceptable User Policy as part of their transition pack. When returned these will be held on their school record. Until this policy has been signed and returned, users will be unable to access or use the school's accounts and IT systems.

This policy should be read in conjunction with:

- Behaviour for Learning Policy
- Data Protection Policy

Sanctions

The details of any serious breach of the rules by students will be dealt with in accordance with the Behaviour for Learning Policy. Using the computer network is a privilege, not a right. For serious breaches of the rules, the right to use the computers and associated systems (including Wi-Fi) may be removed, either temporarily or permanently.

Staff members who fail to comply with this Acceptable Use of ICT Policy may be subject to disciplinary action.

Tony Walker
CHAIR OF GOVERNORS

Matthew Fletcher
HEADTEACHER

1. Definitions

“ICT facilities”: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players, hardware, software, websites, web applications or services, and any device, system or service which may become available in the future which is provided as part of the ICT service.

“**Users**”: anyone authorised by the school to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

“Personal use”: any use or activity not directly related to the users’ employment, study or purpose.

“**Authorised personnel**”: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

“Materials”: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

2. Unacceptable use

The following is considered unacceptable use of the school’s ICT facilities by any users. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school’s ICT facilities includes:

- Using the school’s ICT facilities to breach intellectual property rights or copyright.
- Using the school’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school’s policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, downloading, creating, storing, linking to or sending material that is pornographic, illegal, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its students, or other members of the school community.
- Connecting any device to the school’s ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.
- Using websites or mechanisms to bypass the school's filtering mechanisms.
- Users should not attempt to create, modify or run any executable files or scripts. This includes EXE, BAT and PS1 files.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or ICT Systems Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

3. Staff (including governors, volunteers, and contractors)

3.1 Access to school ICT facilities and materials

The school's ICT Systems Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit must immediately contact the ICT Network Manager or ICT Systems Manager. Staff who require additional access permissions should request this through their line manager who may then request this through the ICT Network Manager or ICT Systems Manager.

All school IT equipment is shared and/or assigned to a specific job role or function. School IT equipment is not owned by any member of staff. Users must treat all hardware and systems with care. Staff must not reallocate any IT equipment without first consulting the IT department.

Any laptops or devices which are provided to a member of staff by the ICT Department must be properly looked after, shut down when not in use, held securely and properly password protected. Staff should not keep devices in open view, for example, in cars.

3.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

Staff should be mindful to maintain a professional tone in all email communication - both internal and external - that upholds the standards outlined in the staff code of conduct and of the School.

If staff send an email in error which contains the personal information of another person or sensitive data, they must inform the Director of Finance & Business Operations and DPO immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.

3.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher or ICT Systems Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with students or colleagues
- Does not constitute 'unacceptable use', as defined in section 3
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that the use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 4.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the school's guidelines on social media and the use of email (see section 4.1.1) to protect themselves online and avoid compromising their professional integrity.

3.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Personal social media accounts should not be used to promote, demote or reference the school in any way.

3.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely. The remote desktop system is managed by the ICT Systems Manager.

Staff accessing the school's ICT 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 ICT facilities from off-site and take such precautions as the ICT Systems Manager may require from time to time against compromising system security. Staff accessing school resources from a personal or public computer must ensure they do not save any passwords and have sufficient anti-virus / anti-malware software installed. The school's IT department can be consulted for advice on this.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

3.4 School social media accounts

The school has an official Facebook and Twitter page, managed by a dedicated member of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

3.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email conversations
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT for a variety of reasons including, but not limited to, the following:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- Provide remote technical support

3.6 Storing sensitive files

Any sensitive files, such as those including personal student and staff information, must be stored securely. These files should be password protected and/or have user-based authentication.

Personal data (including names and images) referring to staff or students must not be stored on personal devices, email accounts or cloud storage unless they are already in public domain, for example on school social media accounts.

4. Students

4.1 Access to ICT facilities

Computers and equipment in the school's ICT suites and learning resource centre are available to students only under the supervision of staff.

Students will be provided with an account linked to the school's virtual learning environment.

Rickmansworth School has e-safety and security monitoring software which notifies the IT Technical Services department if a user behaves inappropriately. Teaching staff have access to view and control student machines in computer suites.

Students are only allowed to print from designated student printers and are only allowed to do so with permission from a member of staff.

4.2 Search and deletion

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

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

All school file storage (including on-site and cloud storage) is only to be used for storing school work. Any inappropriate files (including password protected documents) found may be automatically or manually removed without warning by antivirus software or by the IT department.

4.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the Behaviour For Learning Policy, if a student engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, downloading, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

4.4 Bring Your Own Device ("BYOD")

School digital technology systems are primarily intended for educational use. Users should not run any software or access any websites unrelated to school work while on the school site.

Users should not attempt to log in to someone else's laptop without permission.

Students are allowed to use an approved device within our BYOD scheme for learning. "BYO" Devices must have dedicated security measures in place. The antivirus, firewall and other security measures built-in to Windows 10 or Chrome OS are adequate so users do not need to purchase any additional software for this. Students must not disable the built-in security software on "BYO" devices.

5. Parents

5.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

5.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

6. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

6.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Any system that requires a login should use a complex password. Passwords must be a minimum of 8 characters long, contain at least one capital letter, at least one number, and must not be the user's name.

Personal information in your passwords such as dates of birth should be avoided. Passwords should not be the same as other accounts which the user may access.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Users must not write down any account passwords or access details. If it is necessary to temporarily write down login details, these must be kept in a locked area or secured device and securely disposed of as soon as possible.

6.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

6.3 Data protection

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

6.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT Systems Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT Systems Manager immediately.

Users should always log out of systems or lock their equipment with a password when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

School computers will automatically shut down in the evening and turn on in the morning to reduce power usage and automatically apply updates out of hours.

6.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may use personal devices (including computers and mobile phones) to work remotely, providing there are adequate security measures in place.

If there is a need to take personal data (such as student information) out of school, authorisation must be requested from the ICT Systems Manager and adequate security measures must be used e.g. encrypted USB drives.

7. Internet access

The school internet connection is secured. Staff and students may use their school login details to gain access to the school's BYOD Wi-Fi network. This is only to be used for connecting laptops to the internet for school-related work.

All internet traffic is filtered on-site to block inappropriate material (such as pornographic, criminal, violent, racist or extremist literature). No web content filter is 100% effective so staff or students may occasionally gain access to pages with inappropriate content. If this happens, users must report it to their teacher or the IT department immediately.

Staff and students must not connect personal devices to the school's internet via an ethernet cable. Only Wi-Fi access is permitted for personal devices.

7.1 Students

During a lesson using computers, students may only use websites or software that their teacher has specifically advised they may use for that lesson. They must not have other programs open and must not use the internet unless advised by their teacher.

Users must not download, use or upload any material to the internet which is protected by copyright. Users must seek permission from the owner, before using any material from the Internet. If in doubt, or they cannot obtain permission, material should not be used.

Students must not upload media of themselves, other students or staff onto any school system, nor should they upload images of staff and other students to any website (including social media), without first seeking approval from the individuals concerned.

Students must not attempt to access any sites that are not relevant to school work, including websites that are blocked by the web content filter, such as social networking and games.

Internet chat rooms, social media and streaming websites are strictly banned at school.

7.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the ICT Systems Manager.

The ICT Systems Manager will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

- Visitors need to access the school's 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)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

8. Google Workspace

The school uses Google Workspace for Education, formally known as G Suite for Education. This consists of a suite of collaborative work and productivity tools including Google Docs (word processor), Google Sheets (spreadsheet), Google Slides (presentation) and Google Classroom (assigning classwork).

Data stored in Google Workspace (including Gmail) is not private, is owned by the school and may be accessed by the IT department at any time without permission.

9. Breaches

The IT Department will occasionally monitor published notifications of data breaches. If any are identified, the user will be notified as a password reset will be required immediately. If any staff or student believes their account details have been compromised, they must inform the IT Department immediately.

Every user account will require a password change every 6 months.
To minimize data breaches, users should ensure caution when signing into websites using a school email account and should use different passwords to sign in to different websites. Passwords should not be divulged to anyone else.

10. Social Engineering

Staff must only contact parents or carers via the contact details held within the school's information system (e.g. Progresso or SIMS). Any request to edit or disclose any information relating to staff or students must be communicated via contact details known to the school.

Staff must verify the identity of any staff or student before resetting any login details or granting access to any files, systems or services.

If password resets have to be done remotely, IT staff will ensure that the user changes their password upon next login. This guarantees that the IT staff are not aware of other user's passwords.

Appendix A - Student Acceptable Use of IT Agreement

- I understand that my use of the school's IT systems (including, but not limited to, computers, email, internet, printers) is for educational purposes only.
- I will only access school resources and contact staff from my own school-provided accounts.
- I will ensure that all digital communication with staff, students and the wider school community is professional and appropriate at all times.
- I will not attempt to find or connect with any school staff on social media or similar websites.
- I will not attempt to log in to school systems with credentials other than my own.
- I will not share my account details with anyone or write them down anywhere easily accessible by others.
- I will not use my school email address to sign up for any website or mailing lists that are not relevant to school work. I will not sign up for any websites or mailing lists with anyone else's details.
- I will not attempt to bypass any school e-safety or security systems (including, but not limited to, antivirus, antimalware, web content filter, access control lists).
- I will not attempt to download or install any programs or software on school computers.
- I will not attempt to install or configure any hardware or equipment on the school's systems.
- I understand that any deliberate or malicious act of damage to school equipment or data (physical or virtual) may be classed and processed as criminal damage.
- I understand that my internet browsing history, search logs, emails and more may be stored and monitored on school devices. This may be shared with relevant staff or the police if required and can be used as evidence if school systems have been misused.
- I will not attempt to access, store or distribute any material that could be considered unsuitable, offensive or illegal. If I come across any unsuitable material, I will immediately report it to my teacher or the school's IT department.
- If I think I have been hacked or been infected with a virus or malware, I will contact the school's IT department immediately.
- I will not disclose any personal information (including, but not limited to, name, address, phone number, email address, photographs) of myself or others without clear consent.
- I will not attempt to contact or meet anyone online without permission from a member of staff.
- I will not post any photos or videos online without the permission of all those included in the media.
- I will not attempt to copy, modify or redistribute anyone else's work without permission and will follow all copyright and data protection laws and regulations.
- I will not take secret photos, videos or recordings of teachers or students, including when learning remotely.

- I will not plug in any storage media to school computers (including, but not limited to USB flash drives, hard drives, SD cards, mobile phones and optical media) without permission from the school's IT department.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I have read, understood and agree to the Acceptable Use of IT policy. I understand that this policy may be updated during my time at Rickmansworth School.
- I understand that these rules are designed to keep me and the school safe.
- I understand that access to the school's systems is a privilege, not a right, and failing to follow these rules may result in sanctions including revoking access. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

I have read and understand the rules detailed in the Acceptable Use of IT policy.

Print Student Name:

Student Signature:

Date:

Print Parent / Guardian Name:

Parent / Guardian Signature:

Date:

Appendix B - Staff Acceptable Use of IT Agreement

- I understand that use of the school's IT systems (including, but not limited to, computers, email, internet, printers) has been granted to me primarily for school purposes. I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will only access school resources and contact staff, students, parents and governors from my own school-provided accounts. Under no circumstances are staff to use their personal email address or phone number to contact students or parents. If staff are working remotely and unable to come into school to make calls, they may use their own mobile but they must ensure their personal phone number is hidden.
- I will only email students using the students' school email address.
- I will ensure that all digital communication with staff, students and the wider school community is professional and appropriate at all times and will not be used in a way which could harm the school's reputation.
- I will not attempt to find or connect with any students on social media or any similar websites.
- I will not attempt to log in to school systems with credentials other than my own.
- I will not share my account details with anyone or write them down anywhere easily accessible by others.
- I will not attempt to bypass any school e-safety or security systems (including, but not limited to, antivirus, antimalware, web content filter, access control lists).
- I will not attempt to download or install any programs or software on school computers without permission from the IT Systems Manager.
- I will not attempt to install or configure any hardware or equipment on the school's systems without permission from the IT Systems Manager.
- I understand that any deliberate or malicious act of damage to school equipment or data (physical or virtual) may be classed and processed as criminal damage.
- I understand that it is my responsibility to undertake a basic equipment check in computer labs at the beginning and end of computer lessons and I will report all faults to the IT department immediately.
- I understand that my internet browsing history, search logs, emails and more may be stored and monitored. This may be shared with relevant staff or the police if required and can be used as evidence if school systems have been misused.
- I will not attempt to access, store or distribute any material that could be considered unsuitable, offensive or illegal. If I come across any unsuitable material, I will immediately report it to the school's IT department.
- If I believe my account has been subject to hacking or been infected with a virus or malware, I will contact the school's IT department immediately.
- I will not disclose any personal information (including, but not limited to, name, address, phone number, email address, photographs) of myself or others without clear consent.

- I will not post any photos or videos online without the permission of all those included in the media.
- I will not attempt to copy, modify or redistribute anyone else's work without permission and will follow all copyright and data protection laws and regulations. This includes using pirated or illegally downloaded music and videos and using streaming services (e.g. Netflix, Spotify) to play to an audience.
- I will not plug in any storage media to school computers (including, but not limited to USB flash drives, hard drives, SD cards, mobile phones and optical media) without permission from the school's IT department.
- I will only use the school's management information system for its intended purpose and will only look at data relevant to what I am looking for. I understand that all access to staff, student and parent records is recorded.
- I will not take any sensitive or personal data outside of the school and its network. If there is a reason why data must be taken out, this must be discussed with the school's IT department and stored in a format that is encrypted or password protected.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will take all reasonable steps to ensure that personal devices through which I access the school's remote desktop and Google applications have up-to-date anti-virus and anti malware. I will not save passwords for school applications on personal devices. I will not save any sensitive or personal data relating to the school on personal devices.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a student 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 have read, understood and agree to the Acceptable Use of IT policy. I understand that this policy may be updated during my employment at Rickmansworth School.
- I understand that these rules are designed to keep me and the school safe.
- I understand that failing to follow these rules may result in disciplinary actions including revoking access.
- I understand that I may have access to sensitive data on the school's network and will ensure I lock or log off of any computers I am using before leaving it unattended.
- During remote learning:
    - I will not behave any differently towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a student. The same applies to any private/direct communication with a student.
    - I will not take secret recordings or screenshots of myself or students during live lessons.
    - I will conduct any remote video lessons from home in a professional environment, as if I am in school. This means that the location will be

appropriate and I will be correctly dressed. The background will be professional and appropriate and the camera view will not include any personal information or inappropriate objects.

- I will complete the issue log for live lessons if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students.

I have read and understand the rules detailed in the Acceptable Use of IT policy.

Print Name:

Signature:

Date: