Ravens Wood School

(Part of the Impact Multi Academy Trust)

Policy Document

Policy Name	Acceptable Use of Technology Policy
Date of Last Review:	Autumn 2025
Date of Next Review:	Autumn 2026
SLT Responsible:	Headteacher
Other Staff Responsible:	ICT Manager and Deputy Headteacher
Appendices:	A: Letter to Parents about Personal Technology - Remove A: RWS Student Network Use Agreement B: RWS Staff Network Use Agreement C: RWS Visitor Network Use Agreement
Related Policies:	Bring Your Own Device Policy Mobile Phone Policy Online Safety Policy CCTV Policy Social Media and Networking Policy Impacxt Trust AI policy

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could 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, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school’s policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school’s ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Behaviour Policy and Staff Code of Conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006

- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service or personal devices used in school with the permission of the IT team or Senior Leadership Team.
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools which have not been authorised by the IMPACT Multi Academy Trust (as per the Trust AI policy)
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher, alongside Senior Leaders and the IT manager will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. This would need to be requested on an ad hoc basis.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and staff code of conduct.

Specific sanctions could include:

Students:

- Temporary or permanent ban on Internet and/or computer use in that lesson or subject.
- Users may be charged for the repair or replacement of equipment.
- Parents/carers informed.
- Additional disciplinary action may be taken in line with existing policy on behaviour, language, bullying and exclusions.
- In extreme circumstances, removal of access to the school network may be permanent across all subjects. In this case, arrangements would be made for the student to work on a stand-alone machine.

Staff:

- Referred to the Headteacher/Governors/Trust through school disciplinary procedures.

For further information please see the policies listed at the front of this document (Bring Your Own Device Policy, Mobile Phone Policy, Online Safety Policy, CCTV Policy, social media and Networking Policy, Impact Trust AI Policy)

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

5.1 Access to school ICT facilities and materials

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

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Manager who will confirm with the Higher Senior Leadership team before making any changes.

5.1.1 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. Multi-factor authentication is required to access email account(s).

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/carers and pupils and must not send any work-related materials using their personal email account.

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

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.

If staff send an email in error that contains the personal information of another person, they must inform their Line Manager and IT Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. 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 as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The IT Manager and Headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time directed time or teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils 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 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 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone/personal device policy.

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 pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (Social Media and Networking Policy) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

5.3 Remote access

Staff have access to the network drive via Foldr and this requires multifactor authentication use.

Staff can access Microsoft 365 (including SharePoint and One Drive) off site

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 outside the school.

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.

5.4 School social media accounts

The school has an official Instagram account and WhatsApp Broadcast channel, managed by The Headteacher and Deputy Headteacher. 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 may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

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

The school monitors ICT use in order to:

- 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

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to pupils in Key stage 3 and 4 only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Sixth-form pupils can use the computers in the Learning commons, Library and Hall independently, for educational purposes only

6.2 Search and deletion

Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out (as per the Behaviour Policy), **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos

- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / designated safeguarding lead / appropriate member of staff
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, you should proceed according to your behaviour policy) The authorised staff member should:
- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil 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 making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

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

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

7.2 Communicating with or about the school online

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

Parents/carers 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.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

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

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 pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Passwords will be allocated by the IT manager. These will be autogenerated to avoid unauthorised access to accounts. This applies to staff and students

8.2 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 have these installed, and 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.

8.3 Data protection

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

8.4 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 IT Manager and overseen by the Headteacher and Deputy Headteacher.

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 IT Manager immediately.

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

8.5 Encryption

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the school will verify this using an annual Trust audit
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data, the network drive is backed via a Virtual Machine on a weekly basis (and incrementally n a daily basis), SharePOint and Microsoft 365 is backed up via Baracuda on a daily basis.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the IT Management contract (Turn it On)
- Make sure staff:
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on

10. Internet access

The school's wireless internet connection is secure.

- The school uses Smoothwall to filter the WiFi and LGFL is also filtering
- We have separate WiFi VLAN for staff and visitors and sixth form. They need to log into the WiFi portal to gain access with user credentials from the IT Manager. All access is logged.

10.1 Pupils

Students in Key stage 3 and 4 are not able to use WiFi unless authorised by the Head Teacher or Deputy Head teacher to support with Teaching and Learning.

6th form students can access the WiFi network with their user details

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers 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 WiFi 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 WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher and IT manager and Deputy Headteacher will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for reviewing and approving this policy.

12. Related policies

This policy should be read alongside the school's policies on:

- Bring Your Own Device Policy
- Mobile Phone Policy
- Online Safety Policy
- CCTV Policy
- Social Media and Networking Policy
- Impact Trust AI policy

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening via the neutral notification form

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred – report it via STOP@
- Report the material to the relevant social media company or network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation, disciplinary procedures and behaviour policy are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix A: Acceptable use of the internet: agreement for parents and carers

Ravens Wood School

(Part of the Impact Multi Academy Trust)

Student Network Use Agreement

I understand that the computer network and ICT facilities including Microsoft 365 are provided to benefit my education and agree to keep to the network use rules written below:

- I will only log on using my username and password – I will never log on as anyone else or access other students' work. I will never share my username and password with anyone else.

- I will not try to reach areas of the network that are restricted nor will I attempt to cause damage to the school's network or ICT equipment.

- I will only use the network and ICT facilities for my school work and will not play games, download or install programs or try to reach unsuitable or blocked websites at ANY time.

- If I bring storage devices e.g. flash drives (memory sticks) from home, I will make sure that they contain ONLY school work and understand that the network staff may check these for viruses or inappropriate content etc.

- When writing e-mail and other documents, I will ALWAYS be polite and never take part in online bullying.

- I will use ONLY my RWS email account to communicate with members of RWS staff and never a personal account.

I understand that failure to keep these simple rules or causing deliberate damage to equipment may result in my network access being removed in addition to actions taken in accordance with the school's disciplinary procedures. If I am worried or need help with issues related to this agreement, I know I can talk to the school's Designated Safeguarding Lead, Mr French.

Signed: ____________________________ (student)

Signed: ____________________________ (parent/carer)

Date: __________________

CCTV cameras are in operation in all ICT suites.

Appendix B: Acceptable use of the internet: agreement for staff

RWS Staff Network Use Agreement / ICT Contract

Name:

This document has TWO sections. The first is relevant ONLY if you have been issued with ICT equipment such as a staff laptop and the second refers to ICT equipment, systems and services in general and concerns ALL STAFF.

1. I confirm that I have been issued with the following ICT equipment:

□ 1 Device

□ 1 Power Supply

□ 1 Carry Case/Bag

□ No equipment issued

Please read the following statements carefully – you will be required to sign to affirm agreement and compliance at the end of this document:

With respect to the laptop I have been issued:

- I fully understand that the laptop is the sole property of Ravens Wood School and will be recalled whenever the school deems necessary. I understand that I must comply immediately if such a request is made.

It is strongly recommended that you keep a backup on the school network of any important files at all times.

- I fully understand that the security of the laptop and power supply is my responsibility and I could be liable for the cost of replacement should they be stolen from any location where I haven't ensured appropriate security.
- I fully understand that it is my responsibility to maintain the integrity of my laptop password and the status of its pre-configured anti-virus, anti-spyware or firewall protection.
- I fully understand that damage incurred to the laptop or power supply may not be covered by insurance and I could be liable for the cost of replacement or repair. This includes damage incurred in school, at home or any other location.
- I fully understand that the expected 'working life' of the laptop from new (if cared for properly) is in excess of three years. If the laptop becomes unusable before the end of its normal life expectancy there is no guarantee that it will be replaced.
- I fully understand that the laptop is predominantly for work use and that any personal use must not compromise the capability of the laptop to completely fulfil its intended school function. Any personal software installations or downloads will be removed should they interfere with school systems.
- I fully understand that I am responsible for checking that all files, software or other media stored on the laptop would not compromise my position within the school or cause distress if they were to be viewed by a student or any other associate of the school.
- In the event that I notice any material on the laptop that I consider to be unsuitable for viewing by either students or any other associate of the school, I will immediately inform my line manager and in his/her absence, will immediately inform a member of SLT or the IT Manager.
- I undertake to ensure that my laptop is never left unattended. Should I need to leave it while I am logged on I will always lock it (using the Ctrl-Alt-Delete keys) and understand that I am responsible for any unauthorised access including any content which may be added at such times.

I understand that I am responsible for any unauthorised access made to my laptop through USB devices or from any other media.

- I understand that my laptop has been issued to me with a USB encryption key or an encryption password and that the purpose of this key or password is to 'unlock' the encryption applied to the data stored on my laptop. I understand that this key or password must be protected and kept separate from my laptop whenever it is not being used to unlock the device. I understand that if I lose this USB key or encryption password with the laptop, then the data on my school issued laptop may be compromised. I understand that I will be held responsible should this happen.

2. With respect to all other ICT equipment, systems and services:

- I fully understand that it is my responsibility to maintain the integrity of my network password and any other ICT Infrastructure password my role allows me to know.
- I fully understand that I must not alter the status of pre-configured anti-virus, anti- spyware or firewall protection on any item of school ICT equipment.
- If I am logged on to any Ravens Wood networked computer, I will always lock the keyboard (using the Ctrl-Alt-Del keys) if I leave the computer unattended and understand that I am responsible for any unauthorised access which occurs at these times.
- I fully understand that I am completely responsible for the content of my network user area including Microsoft 365 and that I should check to ensure that there is nothing present that would compromise my position within the school or cause distress to the viewer if viewed by a student or associate of the school.
- In the event that I notice any material that I consider to be unsuitable for viewing by either students or any other associate of the school on any item of ICT equipment I will immediately inform my line manager and in his/her absence, will immediately inform a member of SMT.
- I have read both the school's Acceptable Network Use Policy and BYOD Policy and I know that these can be viewed by clicking the link on the VLE Home Page or on the school's website.
- If I bring any personal ICT equipment into Ravens Wood School e.g. Flash memory drives, I will ensure that they contain no material that could be considered in breach of any part of this agreement and will comply with any content check (e.g. for viruses, illegal software or unsuitable material) that may be requested at any time.
- I understand that I must not store sensitive or confidential school data on any system or service not sanctioned by the school. I will endeavour, whenever possible, to save such data exclusively to the school network and will only store data locally to my encrypted school laptop when absolutely necessary. I will not, under any circumstance, save sensitive or confidential data to memory sticks, other removable media or cloud-based services including, but not limited to, Dropbox, Google Drive or a personal Microsoft OneDrive account. I understand that to do so will likely constitute a breach of the school's Data Protection and Disclosure policy and by extension, the Data Protection Act and, that I will be held responsible.
- If I need to contact the IT Support Department to report a problem with either the equipment I have been issued or with any other school-based IT equipment, I understand I can e-mail help@rws.uk.net or telephone Ext 250.

Declaration:

I have read and understand the preceding statements and discussed this policy with the ICT Manager or member of the ICT Support Staff. I agree to abide by this RWS Staff Network Use Agreement / ICT contract.

Signed: ....

Name (please print): .... Date: ....

ICT Manager: .... Date: ....

ICT Network Agreement Stamp

Appendix C: Acceptable use of the internet: agreement for Visitors

RWS Visitor Network Use Agreement / ICT Contract

Name: _

Please read the following statements carefully – you will be required to sign to affirm agreement and compliance at the end of this document:

With respect to all other ICT equipment, systems and services:

- I fully understand that it is my responsibility to maintain the integrity of my network password and any other ICT

Infrastructure password my role allows me to know.

- I fully understand that I must not alter the status of pre-configured anti-virus, anti- spyware or firewall protection on any item of school ICT equipment.
- If I am logged on to any Ravens Wood networked computer, I will always lock the keyboard (using the Ctrl-Alt-Del keys) if I leave the computer unattended and understand that I am responsible for any unauthorised access which occurs at these times.
- I fully understand that I am completely responsible for the content of my network user area and that I should check to ensure that there is nothing present that would compromise my position within the school or cause distress to the viewer if viewed by a student or associate of the school.
- In the event that I notice any material that I consider to be unsuitable for viewing by either students or any other associate of the school on any item of ICT equipment I will immediately inform my line manager and in his/her absence, will immediately inform a member of SMT.
- I have read both the school's Acceptable Network Use Policy and BYOD Policy and I know that these can be viewed by clicking the link on the VLE Home Page or on the school's website.
- If I bring any personal ICT equipment into Ravens Wood School e.g. Flash memory drives, I will ensure that they contain no material that could be considered in breach of any part of this agreement and will comply with any content check (e.g. for viruses, illegal software or unsuitable material) that may be requested at any time.
- I understand that I must not store sensitive or confidential school data on any system or service not sanctioned by the school. I will endeavour, whenever possible, to save such data exclusively to the school network and will only store data locally to my encrypted school laptop when absolutely necessary. I will not, under any circumstance, save sensitive or confidential data to memory sticks, other removable media or cloud based services including, but not limited to, Dropbox, Google Drive or a personal Microsoft OneDrive account. I understand that to do so will likely constitute a breach of the school's Data Protection and Disclosure policy and by extension, the Data Protection Act and, that I will be held responsible.

- If I need to contact the IT Support Department to report a problem with either the equipment I have been issued or with any other school-based IT equipment, I understand I can e-mail help@rws.uk.net or telephone Ext 250.

Declaration:

I have read and understand the preceding statements and discussed this policy with the ICT Manager or member of the ICT Support Staff. I agree to abide by this RWS Staff Network Use Agreement / ICT contract.

Signed: ………………………………………………………………………….

Name (please print): ………………………………………………………………………. Date: ……………………

ICT Manager ………………………………………………………………………. Date: ……………………

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.