Ravens Wood School

(Part of the Impact Multi Academy Trust)

Policy Document

Policy Name	Bring Your Own Device (BYOD) Policy & Personal Electrical Appliances
Date of Last Review:	Summer 2025
Date of Next Review:	Summer 2026
SLT Responsible:	Headteacher / Business Manager
Other Staff Responsible:	ICT Manager

Contents

1. About this policy

We recognise that many of our staff and students have personal mobile devices (such as tablets, smartphones and laptops) which they could use for school-related purposes, and that there can be benefits the school, staff and sixth formers, including increased flexibility in our working practices, in permitting such use.

However, we have significantly less control over an individual's device compared with our own ICT facilities. Such devices therefore pose a risk to our ability to comply with our legal obligations in respect of personal data and confidential information. For serious breaches of the Data Protection Act 2018, the Trust may be fined by the Information Commissioner's Office and staff may incur personal liability for breaches of the Act.

The school (under the Trust umbrella) is a Data Controller for the purposes of the Data Protection Act 2018 and must remain in control of the personal data for which it is responsible, regardless of ownership or location of the device used to carry out the processing.

Anyone covered by this policy may use a personal mobile device for school-related purposes, provided that they have read this policy, signed the relevant Network Use Agreement and adhere to the terms of both documents.

Whilst the school's on-site facilities for the use of personal devices provide access only to the Internet and prevent access to other network services, in certain circumstances the use of a personal mobile device may allow our staff to access, for example, information about pupils, email communication with staff and parents, photographs, assessments, reports, confidential minutes of meetings, etc. An example of these circumstances would be the use of a personal device on or off site, such as a mobile telephone, to obtain and store school email.

By making information available to mobile devices we are at risk of the devices being lost or stolen, or being shared with individuals who are not authorised to have access to such personal data. For this reason, we require anyone who wishes to use their own mobile device for school-related purposes to accept the terms outlined in this policy, which enables us to take measures where and when necessary including remotely wiping all personal information from the device to ensure that we comply with our legal obligations as a data controller.

No one is required to use their personal mobile device for school-related purposes. It is a matter entirely for each person's discretion.

This policy covers all employees, sixth form students, officers, consultants, governors, directors, volunteers, agency workers, external visitors and the term 'users' is used for the purposes of this policy to include all those roles.

This policy does not form part of any employee's contract of employment and we may amend it or remove the policy entirely, at any time.

This policy does not place any contractual obligations on us.

2. Definition of terms

Personal Data means data which relates to a living individual who can be identified (a) from that data, or (b) from that data and other information which is in the possession of, or is likely to come into the possession of the school, and includes any expression of opinion about the individual and any indication of the intentions of the school or any other person in respect of the individual.

The Representative means either the school's Headteacher and/or ICT Manager.

The School means Ravens Wood School under the Impact Multi Academy Trust.

3. Personnel responsible for this policy

The school's Headteacher has overall responsibility for the effective operation of this policy but has shares day-to-day responsibility for its operation with the ICT Manager. The Representatives shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

The Representatives are responsible for ensuring that any person who may be involved with administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

The Representatives are responsible for ensuring that all relevant individuals within the school have sufficient information and training to implement this and all related policies.

All users are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the Representatives.

If you have any questions regarding this policy or have questions about using your device for school-related purposes, which are not addressed in this policy, please contact the Representatives.

4. Scope and purpose of the policy

This policy applies to users who use a personal mobile device including any accompanying software or hardware (referred to as a **device** in this policy) for school-related purposes. It applies to use of the device both during and outside working hours and whether or not use of the device takes place on school property.

This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, tablets, and laptop or notebook computers.

When you access our systems you may be able to access data which is confidential, proprietary, private or Personal Data relating to pupils, parents, staff, governors and other individuals (collectively referred to as **school data** in this policy). For the avoidance of doubt, school data includes data relating to Ravens Wood School, and any contractor or other party associated with the school.

When you access our systems using a device, we are exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to our systems or school data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of school data (including, but not limited to, personal and confidential information relating to school pupils, all employees, officers, consultants, governors, directors, volunteers, agency workers and external visitors which could expose us to the risk of non-compliance with legal obligations of confidentiality, safeguarding, data protection and privacy).

The purpose of this policy is to protect our systems and school data, and to prevent school data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal in cases involving staff, actions in line with the schools disciplinary policies in cases involving students and in the case of a breach of this policy by a contractor, consultant, casual or agency worker, the termination of the engagement in addition to any necessary legal actions.

Disciplinary action may be taken whether the breach is committed during or outside working hours and whether or not use of the device takes place on school property. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details. It may also lead in some cases to possible criminal charges. You may also commit an offence under section 170 of the Data Protection Act 2018 (section 55 of the DPA 1998) if you knowingly or recklessly without the school's consent:

- obtain or disclose personal data or the information contained in personal data; or
- procure the disclosure to another person of the information contained in personal data.

5. Connecting devices to our systems

Connectivity of all devices is centrally managed by the ICT Manager who in turn, delegates authority to the School ICT Support team, who must either approve a device or provide connection credentials before it can be connected to our systems.

Staff and Sixth Form are able to connect to an on-site wireless network, which provides filtered, monitored Internet access only using their network credentials. Visitors or other users may be issued with temporary login credentials providing access to an on-site wireless network also providing only a filtered, monitored connection to the Internet.

If users chose to connect to the school's email system or VLE environment using a personal device then they will be required to install software and/or managed profiles in order to allow the school to protect our data and systems remotely. The user can remove this software and/or managed profiles at any time but access to our systems will be disabled.

We reserve the right to refuse or remove permission for your device to connect with our systems. The Representatives and/or ICT Support team will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, us, our users, our connections, our systems, or our school data at risk or that may otherwise breach this policy.

Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist staff in connecting to our systems.

6. Monitoring

The contents of our systems and school data are our property. All materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and Internet activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as **content** in this policy) during the course of working on school-related activities or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore you should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate purposes, including, without limitation, in order to:

- prevent misuse of the device and protect school data;
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
- ensure that users do not use our facilities or systems for any unlawful purposes or activities that may damage our cause damage to the school's reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

By signing the Network Use Agreement / ICT Contract and/or connecting a personal device to any of our guest or remote systems you confirm your agreement (without further notice or permission) to such monitoring and to our right when relevant or necessary to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

7. Security requirements

When using your device to connect to our systems or to process personal data relating to school employees, students, officers, consultants, governors, directors, volunteers, agency workers or external visitors you must:

- at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device;
- install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the device and secure its data, including where relevant or necessary, providing us with any necessary passwords;
- protect the device with a pin number or password, and keep that pin number or password secure at all times. If the confidentiality of a pin number or password is compromised, you must change it immediately and inform the Representatives and/or ICT Support Team. Where school data is stored

on the device, additional security measures to access the school data must be adopted including a password that is changed regularly and/or encrypted;

- If other people such as family members have access to your device, ensure that further levels of security such as passwords or encryption are in place and there is adequate security between the school data and other data stored on or accessible via the device
- not alter the security settings provisioned by the school on the device without our consent;
- keep the devices operating system current with security patches and updates;
- not download or transfer any school data to the device, for example via e-mail attachments, unless specifically authorised to do so. Users must immediately erase any such information that is inadvertently downloaded to the device;
- not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of school data without express authority of the school. Any such unauthorised backups created must be deleted immediately;
- where we have permitted you to store school data on the device, ensure that the school data is encrypted using appropriate encryption technologies approved by the Representatives;

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the school data on it for legitimate school-related purposes, which include (without limitation) enabling us to:

- inspect the device for use of unauthorised applications or software;
- inspect any school data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect school data;
- investigate or resolve any security incident or unauthorised use of our systems;
- conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, safeguarding, data protection or privacy); and
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken.
If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any school data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should therefore regularly backup any personal data (excluding any school data) contained on the device.

By signing the Network Use Agreement / ICT Contract and/or connecting a personal device to any of our guest or remote systems, you consent to us, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using some or all of the data on or from a device for the legitimate school-related purposes set out above.

8. Lost or stolen devices and unauthorised access

In the event of a lost or stolen device, or where a user believes that a device may have been accessed by an unauthorised person or otherwise compromised, the user must report the incident to the Representatives or ICT Support team immediately and in any event on the same working day if the incident happens during working hours or on the next day if the incident occurs outside of working hours.

Appropriate steps will be taken to ensure that school data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all school data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from Trust data in all circumstances. You should therefore regularly backup all personal data (excluding school data) stored on the device.

9. Procedure on termination of employment

On your last day of work, or your last day before commencing a period of garden leave, all school data (including work e-mails), and any software applications provided by us will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the ICT Support team for data and software removal. You must provide all necessary co-operation and assistance to the ICT Support team in relation to this process.

10. Personal data

We shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless absolutely necessary. If such access or copying occurs inadvertently, we shall delete any and all such personal data as soon as it comes to our attention. This limitation does not apply to personal data which is also school data (including personal e-mails sent or received using our e-mail system). For this reason, you are encouraged not to use work e-mail for personal purposes.

11. Appropriate use

You should never access or use our systems or school data through a device in a way that breaches any of our other policies. For example, you must not use a device to:

- breach any obligations relating to confidentiality, privacy and safeguarding;
- breach any school policy which applies to you, including our Data Protection and Disclosure policy;
- breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to a device).

12. Technical support

We do not provide technical support for devices. You are responsible for any repairs, maintenance or replacement costs and services.

13. Costs

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs.

You are under no obligation to use, supply or bring with you, a personal device for the purposes of your employment, visit to, or education at the school – as such the school/trust cannot be held liable for any costs associated with loss or damage to the device, regardless of whether or not a Network Use Agreement / ICT Contract has been signed.

By signing the Network Use Agreement / ICT Contract and/or connecting a personal device to any of our guest or remote systems you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your school-related usage of the device may increase your voice and data usage charges.

14. Personal Electrical Appliances

The leads and plugs of personal electrical equipment, or sometimes the equipment items themselves, can be damaged with use, which may result in an accident or electric shock. Faulty items can cause severe and permanent injuries. Damaged equipment can cause fire that can lead to death or injury to others.

To reduce the risks associated with the use of unauthorised personal electrical equipment to staff and students at the school.

Any member of staff wishing to bring a personal electrical equipment item to the school must make a request to the school's Business Manager and receive approval before bringing said item into the school. If it is deemed appropriate for the item to be in school, it will be PAT tested (portable appliance testing) and authorised for safe use. The school reserve the right to remove and dispose of any unauthorised personal electronic items found on site though efforts will always be made to return them to the owner on condition of removal in the first instance.

15. Student's Personal Equipment for Specific Learning Needs (see Appendix 1 below).

Appendix 1

Dear Parent/Carer,

We hope this message finds you well.

As you may be aware, your child has specific learning needs that can impact their access to the curriculum. To better support their learning in the classroom, we believe your child would benefit from using a laptop during lessons.

While the school does have a limited number of devices available, demand often exceeds supply, and unfortunately, we are not always able to provide one for every student who needs it. To help bridge this gap, we are inviting students who are able to do so to bring their own personal laptop to school for educational use.

Please take a moment to read the attached agreement carefully. If you would like your child to bring their own laptop to school, kindly complete and return the signed agreement to the SEN Department at jvs@rws.uk.net. If you have any questions or would like to discuss this further, please don't hesitate to contact us at send@rws.uk.net.

Thank you for your continued support in helping us provide the best possible learning environment for your child.

Warm regards,

Mrs Jacqui Sultana
SEN Department

16. Student Laptop Use Agreement

I agree to my child, __________________, bringing a personal laptop to school for educational use. I understand and accept the following terms:

1. Responsibility and Liability

- The laptop remains the sole responsibility of the student at all times.
- The school accepts no liability for loss, theft, or damage to the device, whether on school premises or in transit.
- The school will not provide technical support, insurance, or storage for personal devices.
- Devices must be taken home daily and must not be left on school premises overnight.

2. Acceptable Use

- The laptop must only be used for educational purposes and in accordance with the school's Acceptable Use Policy (AUP).
- Students must not use the device to access inappropriate content or engage in non-educational activities during school hours.
- Internet access on personal devices will be blocked while on the school network. Students must work offline using pre-downloaded materials or software. Occasionally, IT Support may enable internet access to support learning but this will be a temporary measure.

3. Classroom Use

- Use of the laptop is at the discretion of teaching staff. If it is deemed that the device is not being used appropriately or is not supporting learning, permission may be withdrawn.
- Students must ensure they are taking sufficient notes and completing all required work. Failure to do so may result in the withdrawal of laptop privileges.

4. Security and Data Protection

- Students are responsible for ensuring their device is protected with up-to-date antivirus software and a secure password.
- Devices must not be used to store or share personal or sensitive data about other students or staff.
- The school reserves the right to inspect the device if there is a safeguarding or security concern.

5. Examinations

- Continued use of a laptop as a normal way of working may support future access arrangements for external examinations (e.g., GCSEs, A Levels), subject to JCQ regulations and school approval.

Parent/Carer Declaration

I have read and understood the terms of the BYOL agreement and agree to support my child in adhering to them.

Signed: ___________________________________
Print Name: ________________________________
Date: _____________________________________