# BRING YOUR OWN DEVICE (BYOD) / PERSONAL DEVICES POLICY

| | | | |
|---|---|---|---|
| Prepared By: | David Adcock | Date Adopted: | May /June 2021 |
| Job Title: | IT Lead | Status: | |
| Authorised By: | Kate Grant | Last Reviewed: | September 2023 |
| Job Title: | CEO | Ratified: | September 2023 |
| Reviewed: | Julia Martin | Next Review: | September 2025 |
| Job Title: | IT Manager | Version: | 1.6 |

## TABLE OF CONTENTS

## 1. Purpose

1.1 This policy outlines the use of personal devices connecting to Jigsaw's network or data.

## 2. Definitions

2.1 'Jigsaw' includes Jigsaw Trust, Jigsaw CABAS® School, Jigsaw Plus and Jigsaw Trading 2013 Limited (Café on the Park).

2.2 'Personal devices' include but are not limited to smartphones, tablets and laptop computers owned by Jigsaw staff pupils and clients.

2.3 'MFA' Multi Factor Authentication, the use of a text or app as a secondary means of authentication.

2.4 'V-Lan' means A Virtual LAN. This is a method of segmenting the network for different devices according to their location, function or security clearance.

## 3. Scope

3.1 This policy applies to all Jigsaw staff, pupils and learners.

## 4. Personal Devices

4.1 Personal devices are treated as untrusted because Jigsaw has no control over security, Anti-Virus, patching or downloaded data.

4.2 Personal/untrusted devices can connect to the internet via the appropriate BYOD V-Lan when on site. This gives access to the internet only and the device is excluded from Jigsaw's V-Lan so personal devices can't access data stored on Jigsaw's network.

4.3 Connection to the BYOD V-Lan requires the user to have a Jigsaw account and a Smoothwall certificate to be installed on the device.

4.4 Users are prompted to sign in via a splash screen to gain internet access.

4.5 Personal devices are subject to monitoring and filtering of their internet connection only while connected to the BYOD V-Lan.

4.6 Jigsaw will not be responsible for personal devices either relating to loss, damage or technical support.

4.7 Jigsaw accepts no responsibility for any malfunction of a device or loss of personal data due to changes made to the device while on Jigsaw's network or whilst resolving any connectivity issues.

4.8 At any time, the user may be asked to produce the mobile device for inspection. The purpose of these inspections is to ensure that the employee is following company policy or to assist with an investigation.

4.9 Jigsaw mail accounts may be set up on personal devices.

4.10 MFA is enforced for users accessing mail when the device is not connected to the network.

## 5. Personal Device Use

5.1 No personal devices will be taken into pupil areas in Jigsaw School whilst pupils are on site without prior authorisation from the School Management Team.

5.2 It is prohibited for devices to be taken into toilets, changing rooms, medical rooms and wet rooms at Jigsaw School without prior authorisation from the School Management Team.

5.3 No personal devices will be taken into Learner areas in JigsawPlus whilst Learners are on site without prior authorisation from the Senior Management Team.

5.4 It is prohibited for devices to be taken into toilets, changing rooms, medical rooms and wet rooms at JigsawPlus without prior authorisation from the Senior Management Team.

5.5 No images or videos may be taken or stored of Jigsaw learners or pupils without their / parent's consent.

5.6 No images or videos may be taken or stored of Jigsaw staff without their consent.

5.7 Personal devices holding Jigsaw data e.g., email accounts must be configured with a secure password, PIN and/or biometric feature Passwords or PINs must be unique.

5.8 Devices should not be "jailbroken" or "rooted" * or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user. (*To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software).

5.9 Devices should be kept up to date with manufacturer or network provided patches and security updates.

5.10 Should a personal device be non-compliant; Jigsaw reserves the right to remove access to email or other work-related functionality.

5.11 The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to the removal of functionality.

## 6. In case of Loss/sale or Data breach

6.1 If a user suspects that unauthorised access to company data has taken place via a mobile device, they must report the incident to Jigsaw's Data Protection Officer immediately.

6.2 Users must report all lost or stolen devices to Jigsaw's Data Protection Officer immediately.

6.3 If a device is lost or sold it is the user's responsibility to ensure the device is removed from their MFA account. There are notes on Top Tips or contact IT as soon as is practically possible for assistance.

6.4 Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that Jigsaw data is only sent through Jigsaw's email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Jigsaw's Data Protection Officer immediately.

6.5 The Data Protection Officer is responsible for overseeing data protection within the school so if you do have any questions in this regard, please do contact them on the information below: -

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

## 7. User Acceptance

7.1 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it.

7.2 Signature for the acceptance and agreement to this policy are recorded in your probationary targets matrix.

## 8. Policy Review

8.1 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

8.2 This policy was last reviewed in September 2023.

## 9. Version History

| No. | Date | Amendment |
|---|---|---|
| 1.1 | April 2021 | New Policy |
| 1.2 | June 2021 | Addition of Appendix 1 and appendix 2, addition of DPO contact informaiton |
| 1.3 | Sept 2021 | 4.6 removal of “except where relating to the Trusts business” |
| 1.4 | May 2022 | Interim review, no changes |
| 1.5 | March 2023 | Interim review. No changes. |
| 1.6 | September 2023 | Interim review. No changes. |
| | | |
| | | |
| | | |
| | | |

## 10. Related Legislation & Guidance

| Document/Reference | Copy Location |
|---|---|
| Data Protection Act, 2018 | http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf |
| General Data Protection Regulation (GDPR), 2018 | https://gdpr-info.eu |

## 11. Related Internal Documentation

| Document | Electronic Copy Location |
|---|---|
| Data Protection Policy | Common / MyJigsaw / Policies / Trust |
| IT Acceptable Use policy | Common / MyJigsaw / Policies / Trust |
| Data Breach Policy | Common / MyJigsaw / Policies / Trust |
| Mobile and Smart Device Policy | Common / MyJigsaw / Policies / Trust |
| Photos & images of Pupils Policy | Common / MyJigsaw / Policies / School |
| Laptop Policy | Common / MyJigsaw / Policies / Trust |
| E-mail Policy | Common / MyJigsaw / Policies / Trust |
| Password Policy | Common / MyJigsaw / Policies / Trust |

## APPENDIX 1 - Personal device: Exceptional usage agreement

It is Jigsaw's policy that no personal devices will be taken into pupil areas in the school whilst pupils are on site, without prior authorisation from either Emma Hawkins, Director of Education; Mariann Szabo, Deputy Headteacher or Jayne Lobley, Designated Safeguarding Lead and signed agreement of the device owner to the terms set out below. This agreement must expire at the end of the school day on the day of issue.

| | |
|---|---|
| Date of this agreement: | |
| Staff member / Contractor / Visitor name: | |
| Function (School, TSS, JPlus) or Third-Party Company name: | |
| Contact number: | |
| Personal device required on school premises (model name): | |

Please state in the box below the reason for the requirement for a personal device to be taken into pupil areas in the school whilst pupils are on site.

| |
|---|
| |

I confirm that I have read, understood and agree to abide by Jigsaw Trust's Mobile Devices Policy. I agree to the use of a Cam-block sticker* on my device and understand that this sticker must not be removed for the duration of this agreement.

I understand that, at any time, I may be asked to produce the mobile device for inspection, to ensure compliance with company policy and the terms of this agreement.

| | |
|---|---|
| Signed (staff member / contractor / visitor name): | |
| Cam-block sticker number: | |
| Sticker issued by (SMT member name): | |
| Time sticker issued: | |
| Time sticker checked and removed by SMT (*One of three individuals named above) | |

*The Cam-block sticker completely blocks the camera, so pictures and videos can't be taken. They are different to an ordinary adhesive sticker because they are tamper evident. This means that once the Cam-block sticker is peeled away, VOID text appears across the face of the sticker. As a result, the sticker can't be removed and then reapplied without this being evident.

The Cam-block sticker is completely residue free and, unlike a normal adhesive sticker, does not leave a tacky residue on the device, making it a suitable temporary solution to photography prevention.

## APPENDIX 2: Personal device: Exceptional usage agreement procedures

It is Jigsaw's policy that no personal devices will be taken into pupil areas in the school whilst pupils are on site, without prior authorisation from a member of the School Management Team (SMT), as named below, and signed agreement of the device owner to the terms set out in the Exceptional Usage Agreement.

If there is an exceptional circumstance in which you may need to have your phone with you in pupil areas whilst the pupils are on site, please ensure you follow the guidance below:

1. Inform the DSL (Jayne), Director of Education (Emma), or Deputy Head (Mariann) that you will require your phone and for what reason.
2. Complete the exceptional usage agreement form which can be found here.
3. The member of SMT will make a decision whether to authorise this agreement and will issue a Cam-block sticker to use on the camera function of your device if agreed.
4. Your request will be logged.

*The Cam-block sticker completely blocks the camera, so pictures and videos can't be taken. They are different to an ordinary adhesive sticker because they are tamper evident. This means that once the Cam-block sticker is peeled away, VOID text appears across the face of the sticker. As a result, the sticker can't be removed and then reapplied without this being evident.*

*The Cam-block sticker is completely residue free and, unlike a normal adhesive sticker, does not leave a tacky residue on the device, making it a suitable temporary solution to photography prevention.*

5. As soon as it is possible to be without your mobile device, please return to one of the named members of the SMT who will check the Cam-block sticker and record this agreement.
6. Return your mobile device immediately to an appropriate place, e.g. personal locker, or office outside of pupil area.

As a reminder, you may be asked at any time to produce the mobile device for inspection, to ensure compliance with company policy and the terms of this agreement.