Bring Your Own Device Policy (BYOD)

Intended for	College wide
Last reviewed	August 2025
Next review	August 2027
Reviewed by	Head of IT, UK
Approved by	Principal

1. Purpose and Scope

1.1. Introduction

This policy is designed to support the responsible use of personal devices in College, enhancing and enriching the teaching and learning experience. It also outlines measures to protect students from harm, minimise risks to the Oxford International College (OIC) Brighton network, clarify user responsibilities, define acceptable and unacceptable use under the BYOD policy, and explain the possible consequences of not adhering to the rules

1.2. Scope

This policy applies to all students and staff who bring personal electronic devices onto OIC Brighton premises or connect them to the College's digital systems (on campus or remotely)

1.3. Definitions

BYOD: "Bring Your Own Device"; the use of personally owned devices (e.g. laptops, tablets, mobile phones) for educational or work purposes.

Device: Any privately owned, internet-enabled electronic device.

College Network: OIC Brighton's IT infrastructure, including wired and wireless networks, internet access, and internal systems.

User: is any individual granted authorisation to use BYOD. Users may include students, staff, volunteers, visitors, contractors, or individuals employed by the College directly or indirectly.

2. Acceptable Devices

Permitted devices include:

- Smartphones
- Tablets
- Laptops
- E-readers (for academic use only)
- Smartwatches (in limited, non-disruptive use)

Devices must:

- Be in full working order.
- Be capable of supporting secure connections and updates.
- Not be jailbroken or rooted (to avoid security risks).

3. Permissions and Usage Rules

3.1. Students — Permitted Use

Students may:

- Use devices during lessons only with the teacher's explicit permission.
- Access digital learning resources, emails, research tools, and OIC Brighton platforms.
- Use devices during break or lunch in designated areas, for appropriate activities only.
- Use headphones when required for learning, if authorised by a member of OIC Brighton staff.

3.2. Students — Prohibited Use

Students must not:

- Access or attempt to bypass OIC Brighton's filters or use unauthorised VPNs.
- Use mobile data or personal hotspots while on college premises.
- Use devices for gaming, social media, or messaging during lessons unless directed by a member of OIC Brighton staff.
- Photograph, record, or film other students or staff without clear and explicit consent.
- Share or upload College-related images, videos or content to public platforms without consent.
- Allow others to use their device, or access another person's device or account.

3.3. Staff — Permitted Use

Staff **may**:

- Use personal devices for work-related tasks, communication, lesson delivery and planning.
- Access OIC Brighton systems securely, including email and academic platforms.
- Use approved apps and platforms in line with safeguarding and data protection requirements.

3.4. Staff — Prohibited Use

Staff **must not:**

- Store or access confidential or safeguarding data without encryption or proper authorisation.
- Use personal messaging services (e.g., WhatsApp, Instagram DMs) to communicate with students.
- Allow students to access or use their personal devices.
- Share or store College-related data on non-secure cloud platforms (e.g., personal Dropbox, Google Drive).

OIC Brighton staff should also refer to the Staff Handbook and Code of Conduct.

4. Network and Internet Use

- All personal devices **must connect only** to OIC Brighton's secured, filtered Wi-Fi network.
- Use of the network implies acceptance of this policy and the College's Acceptable Use Policy.

- Devices must not be used to:
    - Disrupt or damage the network.
    - Introduce unauthorised software, malware, or viruses.
    - Access or share extremist, violent, illegal, or age-inappropriate material (as defined under the **Prevent Duty** and College safeguarding procedures).

5. Security, Data Protection and Privacy

- Devices must be secured with a strong passcode, biometric lock or PIN.
- Staff and students **must not store** personal data, student records, or safeguarding information on personal devices unless authorised and encrypted.
- OIC Brighton may remotely restrict or monitor access to its systems from any device.
- The College may inspect or request access to personal devices in the event of:
    - A safeguarding concern
    - Suspected policy breach
    - Cyberbullying or misuse

Such actions will be conducted with due respect to individual privacy and in accordance with the **UK GDPR** and the **Data Protection Act 2018**.

6. Safeguarding, Online Safety, and Prevent

- All users must report concerns about inappropriate content, cyberbullying, grooming, or radicalisation to the **Designated Safeguarding Lead (DSL)** immediately.
- Use of personal devices must never compromise student wellbeing, College security, or compliance with the **Prevent Duty.**

7. Device Responsibility and Support

- Students and staff are responsible for:
    - Keeping devices secure, charged and in good condition.
    - Ensuring regular updates and use of antivirus software.
    - Protecting their data.
- Oxford International College Brighton:

- Will offer **limited technical support** (e.g., connecting to Wi-Fi, login issues).
- Will not be held liable for **loss, damage or theft** of personal devices on college premises.

8. Misuse and Sanctions

Breaches of this policy may result in:

- Temporary or permanent withdrawal of BYOD privileges.
- Confiscation of a device (returned only to a parent/guardian in the case of students).
- Detention, suspension, or exclusion for serious or repeated breaches.
- Referral to safeguarding authorities or police, where appropriate.

9. Related Policies and Documents

- Online Safety Policy
- Acceptable Use Policy
- Staff Code of Conduct
- Student Handbook
- OIC Brighton Safeguarding Policy