Atelier —21—
a revolutionary response to school

BRING YOUR OWN DEVICE POLICY

Updated 20.9.24 by James Ashcroft

Rationale

The use of personal mobile devices, such as laptops, enhances learning, is personalized and student-centered, and meets the expectations of teachers, students, parents, and guardians. At Atelier 21, students and staff are permitted to bring their own personal mobile electronic devices to school for educational purposes. This policy applies only to devices recommended by Atelier 21 as relevant to student learning. Currently, the policy applies to laptops; however, discussions regarding the use of tablets or smartphones can be held with the school. For the purpose of this policy, the term 'mobile devices' includes mobile phones, laptops, iPads, and other portable personal devices.

Aims

To harness student and staff connectivity to personal mobile devices for developing 21st-century teaching and learning skills while fostering digital literacy, fluency, and social responsibility in a safe environment.

Implementation

The increasing availability of personal mobile devices has accelerated the demand for new models of learning. Atelier 21 has developed guidelines and procedures for BYOD that will be communicated to staff, students, parents, and guardians through the school website, newsletters, and the staff share drive as required.

Use of Mobile Devices at School

- Students may use their devices in the classroom and during self-directed learning.
- Students are not permitted to use smartphones during break and lunch times.
- Visitors to the school may use their mobile devices in the following locations:
    - In the classroom with the teacher's permission.
    - Main school office.

Responsibility for Devices

Staff, students, and visitors to the school are responsible for their mobile devices at all times. The school is not responsible for the loss, theft, or damage to mobile devices or storage

media. The school Office must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged. Mobile devices must be turned off in prohibited areas and at prohibited times and must not be taken into controlled assessments or examinations unless special circumstances apply.

The school reserves the right to refuse staff, students, and visitors permission to use their mobile devices on school premises.

Access to the School's Internet Connection

The school provides discrete wireless networks that staff, students, and visitors may use to connect their mobile devices to the Internet. Access to the wireless network is at the discretion of the school, which may withdraw access from anyone it considers is using the network inappropriately. The Atelier 21 wireless network is subject to a web-filtering service that restricts the types of sites that can be visited while on the school network. Additionally, Atelier 21 uses Impero to help keep pupils and staff safe by filtering and monitoring online usage.

Note: The school cannot guarantee the security of the wireless network. Staff, students, and visitors are advised not to use the wireless network for online banking or shopping.

Access to School IT Services

School staff and students are permitted to connect to or access the following school IT services from their devices:

- The school email system (where appropriate encryption technologies have been deployed).
- The school virtual learning environment (Office 365 and 'School Drives').
- Video sites such as YouTube to support classroom learning.
- Official school apps.
- Other educational apps prescribed by teachers.

Students are prohibited from accessing social media sites during school hours or on school premises.

Monitoring the Use of Personal Devices

Please refer to the eSafety Policy for further details on the web-filtering software used.

In addition to the web-filtering software, the school uses Impero, a monitoring and filtering program installed on individual devices. Parental permission for this program is sought prior to installation on pupils' personal devices (Appendix 1).

Impero complies with Ofsted requirements and GDPR legislation. It monitors pupils' online activity and alerts administrators to any prohibited content. Data collected via monitoring will be retained for 60 days before deletion, accessible only to approved administrators, the Senior Leadership Team, and Designated Safeguarding Leads.

Note: Impero monitoring is only active when connected to the school network and is disabled when at home or outside school hours.

Compliance with Data Protection Policy

Staff compliance with this BYOD policy is crucial for the school's adherence to Data Protection laws. Staff must apply this BYOD policy consistently with the school's Data Protection guidelines, including the use of Impero on personal devices.

Support

The school cannot support users' own devices but will offer practical advice where possible. The school takes no responsibility for supporting staff's personal devices, nor is it responsible for conducting annual PAT testing of personally owned devices.

Compliance, Sanctions, and Disciplinary Matters for Students

If a student breaches this BYOD policy, the incident will be referred to the School Agreements Council, where sanctions will be decided. More severe incidents will be escalated to the Head of School.

If an incident indicates that a pupil is suffering or likely to suffer significant harm, the Safeguarding and Child Protection Policy will be followed. The designated safeguarding lead (DSL) will determine whether incidents fall under the Behaviour Management Policy, E-safety, or Safeguarding and Child Protection Policy. Serious bullying incidents will be treated with the utmost seriousness.

Incidents and Response

The school takes any security incident involving a staff member's, student's, or visitor's personal device very seriously and will investigate any reported incidents. Loss or theft of a mobile device should be reported to the school Office first. Data protection incidents must be reported immediately to the school's Business Manager.

Appendix 1

ICT IMPERO MONITORING AND FILTERING AGREEMENT FOR PERSONAL DEVICES

Whilst attending Atelier 21 School, your child may be required to use their personal laptop/computer device for school activities. To ensure pupils' safety online, the school requires that its monitoring and filtering system, **Impero**, is installed on any personal laptop or computer device used at school.

By signing this agreement, you give **voluntary consent** for Impero, the school's monitoring and filtering software, to be installed on your child's device. This system will:

- Monitor internet activity during school hours while connected to the school's network.
- Filter and block inappropriate content to protect pupils, with filtering settings updated regularly.

Please note, **monitoring will only occur during school hours or while connected to the school network**. Impero does not monitor activity outside of school time (such as weekends, holidays, or home use).

This monitoring is in line with the school's safeguarding responsibilities as outlined in the **Children's Act 2004** and **Keeping Children Safe in Education**. Data collected will be minimal and limited to browsing activity on the school network. Data retention will be in line with school policy (typically 60 days).

As this is a safeguarding requirement of the school, **if you choose not to agree**, your child will still be able to access school devices during lessons but will not be permitted to use personal devices at school.

Data Protection:

Impero complies with GDPR requirements. For more information on how data will be collected, processed, and stored, please refer to the school's **Privacy Notice**.

You may withdraw consent at any time by contacting the school. If consent is withdrawn, your child will be restricted from using personal devices at school but can still access school-provided equipment.

Pupil Name:……

Parent Name: …….

Parent signature: ……Date…….