Atelier —21—

a revolutionary response to school

BRING YOUR OWN DEVICE POLICY

To be read in conjunction with:

- eSafety policy
- Safeguarding policy
- Child protection policy
- Admissions policy
- Curriculum Statement
- Behaviour management policy
- Anti-bullying policy
- Preventing and Tackling Bullying (July 2017)
- Cyberbullying: Advice for headteachers and school staff (2014)
- Exclusions policy
- Complaints policy
- Mobile phone use policy

Rationale

The use of personal mobile devices, such as laptops, at school deepens learning, is personalised and student-centred, 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 the purpose of learning/teaching. This policy is applies to only those devices recommended by Atelier 21 as being relevant to student learning. At present our policy applies to laptops only, however, if there is a case for use of tablet or smart phone use this can be discussed 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 the purpose of developing 21st century teaching and learning skills and for 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 and when required.

Use of mobile devices at the 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 time. Visitors to the school may use their own mobile devices in the following locations:

- In the classroom with the permission of the teacher
- Main school office

Staff, students and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss, or theft of, or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. 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 when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

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

Please refer to the Mobile Phone Use policy for further information about the use of personal smartphones within school.

Access to the school's Internet connection

The school provides discrete wireless networks that staff, students and visitors to the school may use to connect their mobile devices to the Internet. Access to the wireless network is at the discretion of the school, and the school 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 whilst on the school network. In addition to this Atelier 21 use the program Impero to help keep pupils and staff safe by filtering and monitoring online usage. More about this program is detailed further on in this policy.

The school cannot guarantee that the wireless network is secure, and staff, students and visitors use it at their own risk. In particular, staff, students and visitors are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

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 the learning in the classroom;
- official school apps.
- Other apps to support learning in the classroom as prescribed by Teachers

Students are **NOT** to access social media sites during school hours or on the school premises.

Students may not use devices to record, transmit, or post photographic images or video of a person or persons during school hours or during school activities, unless otherwise allowed by a teacher and are relevant to the classroom curriculum. Students and visitors should be aware that devices are subject to search by appropriate staff if the device is suspected of a violation of the school rules. If the device is locked or password protected the student will be required to unlock the device at the request of teaching or technical staff. The school's network filters (Impero) will be applied to a student device's connection to the internet and any attempt to bypass the network filters is prohibited.

It is the responsibility of parents, guardians and staff to ensure that relevant up to date anti- virus software is installed on their device. Students, visitors and staff are strongly encouraged to keep devices secured at all times when not in use. No students or staff shall be required to share their devices with others. To avoid loss, theft, and damage, sharing of devices with others is not recommended. Lock codes or device passwords are encouraged.

Students and staff are solely responsible for the care of devices they choose to bring to school. Atelier 21 will not be held responsible (either financially or legally) for lost, stolen, or damaged devices nor for any malware viruses that they may inadvertently acquire via the Atelier 21 wireless network.

Monitoring the use of personal devices

Please refer to the eSafety policy for further details of the web-filtering software Dray Tek used.

In addition to the web-filtering software via Dray Tek, the school uses Impero a monitoring and filtering program which is installed on to individual devices. Permission for this program is sought from parents prior to installation on to pupils personal devices (Appendix 1).

Impero is a professional system that meets all our Ofsted requirements and GDPR legislation and more importantly puts the safety of pupils online first. Whilst connected to the school network it is able to monitor pupils online activity and notify administrators at the school of any prohibited content. Data collected via monitoring will be retained for 60 days before being deleted automatically. Only approved appointed administrators at the school, Senior Leadership Team and Designated Safeguarding Leads will have access to these logs.

Impero is installed under a BYOD environment, that monitoring will only be active once it is connected to the school network. This means that all monitoring is disabled when at home, during holidays and weekends and no one is able to access the laptop through Impero whilst disconnected from the school network. Impero is unable to sift through computer files and folders.

All laptops in school must have Impero installed on to them to be able to connect to the school network. Home monitoring programs are not a suitable alternative. Any laptop that does not have Impero installed on to it will not be able to connect to the school network. It is a breach of this policy if a device is used without Impero installed or if Impero has been removed from a device without permission.

If a child leaves the school permanently Impero can be removed from the device by contacting the school IT consultant.

Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the school's compliance with the Data Protection laws. Staff must apply this BYOD policy consistently with the school's Data Protection guidelines. This includes the use of Impero on personal devices.

Support

The school cannot support users' own devices but will offer advice to users in their use where practically possible. The school takes no responsibility for supporting staff's own devices; nor has the school a responsibility for conducting annual PAT testing of personally-owned device.

Compliance, Sanctions and Disciplinary Matters for students

If a student is to be found in breach of this BYOD policy and depending of the severity of the breach, the incident will be taken to the School Agreements Council whereby sanctions will be decided accordingly. If the incident warrants more severe sanctions this will be referred to the Head of School.

Where the 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 decide if incidents are dealt with under the Behaviour Management Policy, E-safety and/or Safeguarding and Child Protection Policy. Any incidents involving serious bullying, hazing, banter or peer-on-peer abuse will result in all parties being deemed to be at risk.

Cyber bullying is taken very seriously, and pupils are made aware that cyber bullying in or outside of school is unacceptable. Pupils are taught how to use digital technology safely and they are encouraged to report any incidents to staff- see E-safety Policy.

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 always investigate a reported incident. Loss or theft of a mobile device should be reported to the School Office in the first instance. Data protection incidents should be reported immediately to the school's Business Manager.

Document Control Information			
Author	Danni Hayes	**Status**	Approved
Version	1.0	**Date**	3/11/2021
Approved by	Hayley Peacock	**Signed**	HPeacock .
Approved Date	3/11/2021	**Review Date**	1/08/2021
Location	https://atelier21schools.co.uk/parents/#Policies		

Document Review			
Version	**Amendment**	**By**	**Date**
1.0	Initial Release	Danni Hayes	3.11.21

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 to carry out school activities. To ensure that pupils are protected at all times the school requires that the school monitoring and filtering system, Impero, is installed on to any personal laptop/computer device which is used at the school.

By signing this agreement, you give consent to having Impero, the schools monitoring and filtering software installed on to your child’s device. This will allow the system to monitor pupils on the internet and filter and block inappropriate content which is updated monthly, keeping pupils safe at all times.

As this is a safeguarding requirement of the school, please note that by not agreeing to this your child will not be able to use their personal laptop/computer device at school.

Pupil Name:………………………………………………………………

Parent Name: ……………………………………………………….

Parent signature: …………………………………………………

Date………………………………………………………..