Definitions:

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>BISC</td>
<td>The use of BISC within this document refers to the Bader International Study Centre and its subsidiary Hertsmonceux Castle Enterprises Ltd.</td>
</tr>
<tr>
<td>Mobile device</td>
<td>Any portable computing device such as a smartphone, laptop or tablet computer.</td>
</tr>
<tr>
<td>Personal data</td>
<td>GDPR defines personal data as “means any information relating to an identified or identifiable natural person (‘data subject’)”</td>
</tr>
<tr>
<td>Work-issued mobile device</td>
<td>Any mobile device paid for by the BISC and given to staff and faculty for the purposes of work.</td>
</tr>
<tr>
<td>Bring your own device</td>
<td>Any mobile device not paid for by the BISC but used by staff and faculty for both work and personal uses.</td>
</tr>
</tbody>
</table>

Purpose:

The purpose of this policy is to detail the appropriate use of mobile devices, including:
Providing guidance on acceptable professional uses of mobile devices to ensure their use does not compromise the BISC or its employees in any way.
Ensuring the security of the information held on mobile devices by minimising the threat of accidental, unauthorised or inappropriate access to the information.

Scope:

This policy applies to all staff and faculty of the BISC who connect to the BISC’s computer network either wired or wirelessly in order to carry out work-related functions, using either a work-issued device or their own device.
Policy:

Work-issued mobile devices

The following section of this policy refers specifically to mobile devices (laptops, tablets and phones) issued by the BISC to support the work activities of staff and faculty. Hereafter, these work-issued devices are referred to as devices or mobile devices.

Provision of work-issued mobile devices

It is the responsibility of managers to determine who of their team require mobile devices and to fund their purchase. BISC IT will supply the device most suited to the needs of the recipient from a limited range of options. All devices will be Android; Apple products are not offered as part of the range. IT will provide training in the use of Android devices for anyone unfamiliar with them. Any mobile devices purchased by departments outside of this process will not be supported by IT.

Recipients of devices must sign a release form to acknowledge that they have read and will abide by this policy. They will be given a copy of this policy for future reference.

All devices remain the property of the BISC and IT reserves the right to return to factory settings the device of any recipient who does not abide by the policy.

Managers must not reallocate devices to new members of their team without notifying IT, as IT needs to maintain a record of changes in ownership.

Managers are responsible for ensuring all devices and accompanying peripherals are returned to IT at the end of an employee’s contract with the BISC. The device must be returned in a condition similar to that provided, with a reasonable allowance for usual wear and tear. Departments will be charged for the replacement of damaged or unusable devices.

All mobile phones will be issued under the calls and data package currently agreed with the service provider contracted to supply the BISC. Line managers are responsible for monitoring the usage made of phones and the accuracy of monthly bills. Calls made within Europe are part of the package. However, calls in other parts of the world are made at additional cost and line managers must agree to these additional charges before phones are used abroad.

Damage to and loss of device

Staff must not leave unattended any device. Loss of a device must be reported promptly to IT so that they can quickly secure or delete the data on it. IT will report the loss to the mobile phone provider who will lock it. IT will also report the loss to the BISC Data Protection Officer (DPO) so that potential data breaches can be investigated and a record made of the incident in case of future data breaches.

IT will label all devices with a unique identifier and return address. Recipients must not remove the label.
Devices must not be taken out of the UK without permission from IT or a member of the Senior Management Team.

**Access to content**

All content created for work purposes on work-issued devices is owned by the BISC (with the specific exception of course content created by instructors). The BISC has the right to request access to the data, and to download and store it on its central servers.

Work-issued mobile devices must not be used to take photographs of individuals without their express written permission. Photographs including identifiable individuals must not be posted on the internet through any medium without the written consent of the individuals concerned.

**Acceptable use**

Work-issued mobile devices are supplied for work purposes. Occasional and incidental personal use in accordance with BISC IT’s Acceptable Use Policy is permitted. Devices must not be used for accessing illegal websites, chat lines, phone voting, gambling or any other activity which puts at risk the reputation of the BISC. Costs incurred during the use of devices for personal use will be paid by the user.

**Data Security**

BISC IT reserves the right to recall any work-issued mobile device in order to apply security updates and patches, antivirus software or other system updates to ensure an adequate level of security.

IT use Microsoft mobile device management (MDM) software to monitor and manage the security of all devices. In the event of the loss of a mobile device they will block further access to the device and will reset the device to factory settings (removing all data) or will remove at minimum the business data.

**Mobile phones and tablets**

All work-issued mobile phones are supplied with PINs and encryption as standard. Staff must not change PINs or accounts on the devices. If a change in PIN is required, the staff member must either bring the device to IT or notify IT of the new PIN.

**Laptops**

All laptops which connect to the domain are issued with a login.

**Storage devices**

IT will issue USB sticks and external hard drives that are password protected and encrypted. Staff must not use unencrypted USB devices.
Bring your own mobile devices

Many staff and faculty choose to use their personal mobile devices for work-related purposes. The BISC encourages staff and faculty while on campus to use desktop PCs provided by IT. The second half of this policy sets out the expectations of the BISC in relation to the security of personal devices used for work purposes.

Data Security

Bring your own mobile device (BYOD) users must be familiar with the security features of their devices. They must ensure that all laptops are password protected (with accounts unique to the employee and not shared with members of their household), have up-to-date antivirus software and regular system updates. Phones and tablets must have PINs and encryption enabled. Passwords and PINs should not be divulged to anyone else.

Logins and passwords to key systems, apps and websites accessed via the devices must not be stored within Windows.

Staff must regularly delete work-related documents and emails on personal devices, keeping for the minimum time possible anything created for a work purpose. Where possible, all work-related documents should be stored on OneDrive or an encrypted USB device. At the very least work documents should be uploaded to the BISC central servers at regular intervals.

Staff must report the loss of any BYOD that contains work-related data to IT as soon as possible. IT will then report the loss to the DPO in case of future data breaches.

Before disposing of any personal device which has been used for work-related purposes, staff must completely remove all work data, either by taking the device to IT for them to wipe the data, or by using a third party and obtaining proof of proper disposal of the device.

Monitoring and access

BISC IT will not monitor the use of BYOD. However, the BISC reserves the right to request access to any work-related data on any device and to retrieve a copy of that data.

BYOD that pose a risk to the security of BISC data will be prevented from accessing the BISC network.
<table>
<thead>
<tr>
<th>Contact Officer(s):</th>
<th>Responsible for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job title</td>
<td>Librarian and Head of Learning, Information and Communications Resources</td>
</tr>
</tbody>
</table>

**Date for Next Review:** 01/05/2021

**Related Documents:** .

**Superseded by:** .