Bring Your Own Devices and Acceptable Use Policy (Staff)

School Details :	**The Island Project School** DofE Registration Number : 334/6010 School Registration Number : 5924196 Registered Charity Number : 1119034 Telephone Number : 01675 442588
Designated Safeguarding Lead :	**Sarah Gallagher –** School Principal Mobile : 07971 543 832 Email : s.gallagher@ipschool.co.uk
Deputy Designated Safeguarding Lead :	**Nicole Sheehan** – SLT (Head of School) mobile: 07971 543 755 email : n.sheehan@ipschool.co.uk **Melanie Collett** – SLT (Head of Further Education) Mobile : 07971 543 753 email : m.collett@ipchool.co.uk **Nial Al-Zanki** – Head of Post 16 telephone : 07971 543 428 email : n.al-zanki@ipschool.co.uk
Designated Trustee For Child Protection:	**Jacqui Walters-Hutton** email : jwaltershutton.trustee@ipschool.co.uk
Senior Leadership Team :	**Sarah Gallagher** – SLT (School Principal) **Carol Howe** – SLT (Curriculum Director email : c.howe@ipschool.co.uk **Nicole Sheehan** – SLT (Head of School) **Melanie Collett** – SLT (Head of Further Education)
Trustees :	**Gordon Booth :** Gbooth.trustee@ipschool.co.uk **Jacqui Walters-Hutton** **Claire Browning** Cbrowning.trustee@ipschool.co.uk **Lucy Doble** ldoble.trustee@ipschool.co.uk
Date Last Reviewed :	Reviewed and reissued : 10th August 2018
To be reviewed by :	10th August 2020

1. INTRODUCTION

1.1 IT and Communication plays an essential role in the conduct of our business. The IT infrastructure including e-mail and internet access have therefore significantly improved business operations and efficiencies.

1.2 The Island Project ("the School") provides laptops for use by Staff (which includes employees, contractors and trustees) to enable them to carry out their roles within School.

1.3 However, some staff members may use their own laptops or other devices for work purposes.

1.4 Smart phones are provided for members of the Senior Leadership Team for work purposes. However, staff members may use their own devices to access the School's Google Drive and email system.

1.5 The School recognises that staff find the ability to use their own devices to access work emails and documents helpful. However, staff must recognise that in doing so, they also have a duty to act responsibly and that they must comply with the terms of this policy.

1.6 Bring your own devices (BYOD) is, however, an increasing trend within the workplace, and this policy is put in place in recognition of this trend.

1.7 This policy is intended to address the use in the workplace by Staff of non-School owned electronic devices such as smart phones, tablets and other such devices to access and store information.

1.8 It is the policy of the School to place as few technical restrictions as possible on the use of personally owned devices. However the use of non-school owned devices to process school information and data creates issues that need to be addressed particularly in the area of data security.

2. STAFF RESPONSIBILITY

2.1 As a member of Staff you are required to assist and support the School in carrying out its legal and operational obligations with regard to data and information stored on your device. You are expected to play your part in maintaining the security of data and information that you handle.

2.2 Staff agree to a general code of conduct which recognises the need to protect confidential data that is stored on, or accessed using, a mobile device, whether that device is provided by the School or is owned personally by the staff member

2.3 This general code of conduct includes, but is not limited to :

- Doing what is necessary to ensure the adequate physical security of the device;
- Maintaining software configuration of the device, both the operating system and the applications installed;
- Preventing the storage of sensitive school data in unapproved applications on the device;

- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes;
- Reporting a lost or stolen device immediately;
- Complying with all other School policies;

2.4 The School is committed, as Data Controller, to treat all personal data fairly and lawfully. As a member of Staff, you are required to:

- Comply with the Data Protection and Data Breach Policy;
- Comply with any subject access requests or other freedom of information requests and you may be required to search your device and provide information requested to the Data Protection Officer;
- Ensuring that any information is processed in accordance with the School's Data Protection and Data Breach Notification Policy.

2.5 Personally owned devices

- The personal smartphone and tablet devices are not centrally managed by the School. For this reason support needs or issues related to a personally owned device is the responsibility of the device owner.
- Specifically the Staff member is responsible for :
    - Ensuring that all content and information have industry standard security passwords in place and that this security mechanism is used to protect that data;
    - settling any service or billing disputes with the carrier;
    - Purchasing any required software not provided by the manufacturer or wireless carrier;
    - Device registration with the vendor and/or service provider;
    - Maintaining any necessary warranty information;
    - Battery replacement due to failure or loss of ability to hold a charge; and
    - Installation of software updates/patches.

When using personally owned devices during the work day, Staff may only access computer sites, internet sites and apps which are relevant to their role within School. If in doubt, they should check with a member of the Senior Leadership Team

2.6 When using their own devices for work purposes, Staff should always create documents directly into the School's Google Drive which is compatible across devices.

2.7 Staff using personally owned devices may not use the School's wifi to access pornographic or other inappropriate websites such as sites which give access to or contain:

- Violence or criminal behaviour;
- Dating websites;
- Attempt to impose or promote extremist views or practices on others;
- Promote anti-British views; and
- Materials which use "hate" terms to exclude others or incite violence.

2.8 Filters are in place to prevent access to any such websites and staff must not attempt to evade these filters.

2.9 Staff must not upload, download or otherwise transfer onto any School systems any inappropriate material as detailed above.

2.10 Staff must not upload any material onto School systems which may result in any breach of copyright or which may introduce any malware into school systems.

3. SECURITY POLICY REQUIREMENTS

3.1 Staff responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited.

3.2 Staff are forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.

3.3 Staff should ensure that access to any personally owned devices are password protected and that other individuals are not allowed to access any School data stored on these devices if they do not work at the School

4. WIFI ACCESS TO SCHOOL NETWORK

4.1 Staff members who connect to the network with a personally owned device will be allowed access to the School systems and resources available via the internet subject to the terms of this policy

5. LOSS, THEFT OR COMPROMISE

5.1 If the device is lost or stolen or it is believed to have been compromised in some way, the incident must be reported **immediately** to a member of the Senior Leadership Team.

5.2 The School will immediately take steps change passwords to emails and accounts, wipe any information relating to the School using the Google Data Removal Tool to remove access to information stored in the School's Google Drive, Server and emails. Annexure 1 sets out the steps which will be taken.

5.3 If any personal mobile device which has been used to access School systems is passed on or sold by any staff member, they **must** ensure that all information stored (including any cache) is removed and that access to school systems is no longer accessible before handing over

6. ACCEPTABLE USE

6.1 This document outlines the key points of our acceptable use policy ("AUP") . It has been written to ensure all adults working within school are aware of the rules

6.2 All members of staff have a responsibility to use the School's IT infrastructure in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All Staff members should note that the School network it is monitored on a regular basis.

6.3 Whilst our network and systems are organised to maintain the most secure environment possible it is your responsibility to make sure the children you are directly working with are safe.

6.4 Software and Downloads:

- Staff members must virus check any USB device storage devices before using on the network.
- No data should be transferred or stored on USB storage devices unless they have been encrypted. The School Principal has a stock of encrypted USB devices for sending information home to pupils
- No software should be downloaded or uploaded to the School's network without discussion with the IT Specialist.
- Copyright and intellectual property rights must be respected when downloading from the internet.

6.5 Email:

- All members of staff are provided with a school email address for communication both internally and with other email users outside of School.
- No member of staff must use non-school email accounts for any school/work related activity
- Staff members are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public. Senior members of staff who correspond directly with outside professionals should, wherever possible, use encrypted methods such as Egress to do so
- E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
- E-mail attachments should only be opened if the source is known and trusted.

- Staff members ensure that all login credentials (including passwords) are not shared with any other individuals, displayed or used by any other individual. If a member of staff believes that has learned their password they will contact the IT Specialist to arrange for this to be changed.

- Any unsuitable communications received must be reported to a member of the Senior Leadership Team immediately.

6.6 Pupil designated IT equipment :

- Staff are not permitted to use any IT equipment which is designated for the use of pupils to access anything which is not directly related to the teaching or reinforcement protocols for pupils.

- Staff must not use pupil designated IT equipment to browse sites (such as gaming sites or YouTube), apps, websites or use for other prohibited purposes as outlined in this policy. Many of our pupils will use browser histories to access sites or uploads on sites such as YouTube, and staff members using pupil designated equipment to access these or other sites constitutes a safeguarding risk.

7. ENFORCEMENT

7.1 Any Staff member found to have violated this policy may be subject to disciplinary action including, but not limited to:

- Account suspension;
- Revocation of device access to the School network;
- Data removal from the device; and/or
- Disciplinary advice and potential termination of employment.

7.2 There should be no expectation of privacy with respect to the use of any electronic device by members of Staff whilst accessing the internet (or accessing files or applications) during working hours and whilst on School Premises.

7.3 The School reserves the right to monitor and restrict internet usage by all Staff either using School equipment or using personally owned devices to access wifi, internet or other School infrastructure.

7.4 In exceptional circumstances, the School may require to access school data and information stored on your personal device. In those circumstances, every effort will be made to ensure that the School does not access the private information of the individual.

7.5 When any member of staff leaves employment, all data will be wiped from any personally owned device using the Google Data Removal Tool to remove access to information stored in the School's Google Drive, server and emails.

7.6 All staff are expected to sign to say that they have read and understand their obligations under the terms of this policy.

7.7 Any breach of this policy may constitute gross misconduct.

ANNEXURE 1

Steps to be taken in case of loss/theft of a personal device

1. Staff member to notify a member of the senior leadership team immediately of loss or theft.

2. The School Principal/IT Specialist will immediately ensure that the Data Removal Tool is enabled to wipe any information from the lost/stolen device.

3. Email and other passwords will be changed immediately.

4. The Staff member will be requested to notify the police.

5. The Data Protection Office will record the loss/theft as a data breach in accordance with the School's Data Protection and Data Breach Policy.

6. The Data Protection Officer will consider whether it is necessary to notify the ICO of the data breach.