BRING YOUR OWN DEVICE ACCEPTABLE USE POLICY

This policy must be read in conjunction with Metanoia Institute's (the Institute) Data Protection Policy, IT and Telephone Acceptable Use Policy and Disclosing Data to Third Parties guidance since all four are closely inter-linked.

1. Policy Statement and Scope

1.1. Consumer electronic devices such as smart phones and tablet computers have seen a huge rise in popularity, available features and capability. Many data controllers are faced with demands from employees, board members or even clients wishing to use these devices in the workplace to carry out their jobs. This might mean that individuals' own devices are used to access and store corporate information, as well as their own. This trend is commonly known as 'bring your own device' or BYOD.

1.2. The specific feature of BYOD is that the user (staff or student) rather than the Institute owns, maintains, supports and safeguards the device on which personal / personal sensitive data is stored or transferred.

1.3. As **'data controller'** the Institute has ultimate responsibility under the General Data Protection Regulation (GDPR) to guard against unauthorised or unlawful processing of personal / personal sensitive data on these devices, whilst inevitably having little control over their use and the degree of security measures in place.

1.4. The aim of this policy is to strike a balance between permitting the use of personal devices in recognition of the need for this; while ensuring that these security measures in place are sufficient to comply with the 6 Principles of Data Protection set out in the GDPR and in particular, **Principle F – Personal Data / Personal Sensitive Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

1.5. This is by no means an easy undertaking and there is no 'one size fits all' solution to information security. The Institute therefore needs to limit this risk by giving specific guidelines and restrictions to ensure that users **adhere to an acceptable use policy** while employed (staff) or on a placement (students).

1.6. In turn, the Institute's staff and students **as 'data users'** have a shared responsibility to make sure that they are fully aware of the implications of using personal devices and that they act with due caution in accordance with the Institute's guidelines.

2. Important Considerations

2.1. The following variables can arise with the use of personal devices:

- data could be stored on a mobile phone, digital recorder, laptop, I-Pad, home computer; or storage media such as a USB stick or memory card;
- data could be stored in several places at once, such as in document files, emails, apps, cloud services;
- data might have been deleted but still recoverable;
- levels of security will differ widely (e.g. anti-virus; firewall and keeping these up to date);
- the use of public Wi-Fi with unrestricted access can further compromise security;
- possibility of use by other household users; how restricted is access to the device itself? are there separate locations for personal and business-related information?
- the more places that data is stored, the more challenging it will be retrieve the data if it is later on part of a 'subject access request' by the data subject or as part of a court subpoena.

2.2. Taking personal data off-site should be considered a short-term measure. No personal data should be taken off-site without authority and having first considered its security. To that end, users are required to observe and adhere to the following principles in order to secure the personal/personal sensitive data stored in their device.

DEVICE SECURITY

- limit the choice of device you use to those which you have assessed as providing an appropriate level of security for the personal data being processed;
- register your device with a remote locate and wipe facility to maintain confidentiality of the data in the event of loss or theft;
- make sure you are able to quickly and effectively revoke access to the device in the event of loss or theft;
- ensure that vulnerabilities in the operating system or other device software are appropriately patched or updated **to avoid placing personal / personal sensitive data processed in your device at risk**;
- do not use 'root' or 'jailbreak' processes on your device as these may remove the default security controls of its operating system, placing the personal data you hold at risk of unauthorised and/or unlawful access;
- use only verifiable and trusted third-party software sources to install apps on your device;
- ensure safe and secure disposal of personal data held on mobile devices as soon as the work is completed and before the device is transferred or sold to a third-party;

DATA STORAGE

- personal / personal sensitive data processed on behalf of the Institute must be held completely separate from data used for personal purposes;

- avoid saving multiple copies of records and restrict the data you store off-site to what you need for that business task; anonymising where possible the information by removing personal / personal sensitive data;
- use strong passwords and where appropriate a PIN to protect the data and change it regularly; and encryption to store it on a device securely;
- log in and out of the cloud service where the personal data may be stored between sessions - remember that loss or theft of the device is not the only means by which unauthorised or unlawful access may occur;
- ensure that access to the device is locked or data automatically deleted if an incorrect password is entered too many times; and/or the device automatically locks if inactive for a period of time;
- **do not** save personal data onto your mobile device's memory card;
- verify the security of additional app protection features to sandbox or ring-fence data;

DATA TRANSFER

- disable interfaces which may be used to connect to other devices as they place a risk on the security of the personal data you hold in the device e.g. public Wi-Fi or Bluetooth to connect to wireless devices such as printers or keyboards
- transfer personal data via an encrypted channel to offer maximum protection;
- do not use public cloud-based sharing or public backup services;

3. Guidance for Users on Acceptable Devices

3.1. The ICO advises against using devices containing personal data while in public places if devices are connected to public Wi-Fi spots e.g. in cafes or hotels. Therefore, the Institute does not allow staff as 'data users' to hold personal / personal sensitive data from its staff and students when using wireless networks which are unprotected.

Staff

3.2. Staff who wish to use their laptop or mobile device in a public place for personal use must ensure they have transferred all personal / sensitive personal data to a secure desktop computer or back up hardware, left securely at home or in the office.

3.3. Staff should use the SharePoint and/or One Drive applications from their Institute's Office 365 online account to store information, making sure they restrict any data stored off-site to what is needed for a given business task; and anonymising where possible the information by removing personal / personal sensitive data.

3.4. The following additional principles must be adhered to by staff while working and/or accessing personal data off-site:

- do not copy personal data unless absolutely necessary;
- never store personal data on a mobile device or home computer unless necessary and the device has been encrypted;

- do not store or transfer personal data where there is a risk that it will be lost or exposed e.g. on unencrypted USB drives, mobile devices or laptops;
- log off or lock your device when away from it or not in use;
- only use your Institute's email account to deal with Institute related business and log off the account when not in use;
- do not use the Institute's email account, SharePoint or OneDrive whilst on transit to the office, home or elsewhere to avoid accidentally disclosing personal data to unauthorised individuals;
- change your password frequently and adhere to the Institute's IT and Telephone Acceptable Use Policy;
- keep hand-written records in a secure place which can only be accessed by you;
- shred paper files and securely erase/delete data before disposing of or transferring your device to a third-party.

Students on placement

3.5. Students who wish to use their laptop or mobile device in a public place for personal use must ensure they have transferred all personal / personal sensitive data to a desktop computer or back up hardware left securely at home.

3.6. Hand-written records must be held in a secure place at home which can only be accessed by you as the appropriate executor.

3.7. Only retain client name and contact details for as long as necessary while you are working with the client. Use the placement organisation's referencing system or pseudonym to log your clinical hours and/or when referring to them in any of your academic assessments.

3.8. Student/practitioners who are in private practice are responsible for ensuring that they are fully compliant with the GDPR and for the security of their clients' personal data.

Digital Recording of Client Sessions

- **Permitted Portable Device**: Encrypted digital recorder is recommended as the safest means of recording and protecting client sessions. These cost around £300.

- **Alternatively**, an encrypted USB Memory Stick to use with an unprotected digital recorder is a much cheaper option but the following additional considerations need to be weighed up:

  - ✓ you would need to transfer the data onto the encrypted memory stick as soon as possible after your sessions, and before travelling to a different location, to ensure that you are not carrying around an unprotected digital recorder with data on it;

  - ✓ the ICO advises against the use of USB sticks, even encrypted, as they are more easily lost given their size. However, for students who do not have long to go before

completing their training or due to financial constraints, careful use of an encrypted USB stick can be a viable alternative;

- ✓ it is not permissible to use your mobile phone unless the phone in question is to be used for recording only and for no other purpose AND the phone has a high level of protection;

- ✓ the recorder should be returned to the practitioner's home as soon as possible after the client session.

Storage of any written material (assessments; case ending summaries; client notes; transcripts of client session recordings)

- **Permitted Device**: desktop or laptop Computer

  - ✓ password protect the desktop or laptop
  - ✓ password protect the documents
  - ✓ if family members have access to the same hardware, keep a separate access for yourself
  - ✓ store documents only in one place
  - ✓ if sending or receiving assessments or case summaries, please retain emails in a designated sub-folder of your inbox so this is readily accessible and ensure that the document is still password protected.

Transferring sensitive personal data

- **Permitted Device:** Encrypted USB Sticks

  - ✓ the ICO strongly advises against the use of storage media such as USB sticks and SD cards because they are more easily mislaid;
  - ✓ the Institute does not therefore permit the use of USB / SD cards for storing information of any kind relating to clients.
  - ✓ per Digital Recording of Client Sessions above, it is acceptable to use encrypted USB / SD cards or equivalent to transfer data from unprotected digital recorders before transporting it to your home/practice.

Date of Revision	June 2019
Author(s)	Amalia Sexton on behalf of GDPR Task Group
Date of publication	23 May 2018
Senior Management sponsor	Chief Executive Officer