Barnardo’s
Corporate Policy

Using Smart Mobile Devices on the Corporate Network

Date:	1st October 2014
Review Date:	30th September 2017
Policy Owner:	Information Security Office – IS Department
Distribution:	Internal. Non-confidential

Purpose

This policy is to govern the use of private and corporately owned smart mobile devices that are connected to Barnardo’s corporate IT network.

Policy objectives:

1. To safeguard the security of Barnardo’s corporate IT network and corporate applications, when accessed through the use of smart mobile technology.

2. To govern the use and management of smart mobile devices, and safeguard the data they hold.

3. To mitigate the information and security risks, associated with mobile devices including:

    a. Loss, disclosure or corruption of corporate data on mobile devices.

    b. Incidents involving threats to compromise of, Barnardo’s IT systems and other information assets (e.g. malware infection or hacking)

    c. Non-compliance with applicable laws, regulations and obligations.

4. Encourage users to understand their own responsibility, for protecting Barnardo’s network, equipment and corporate data.

5. Continue to protect Barnardo’s intellectual property-rights, for corporate information created, stored, processed or communicated on devices in the course of work for Barnardo’s.

This policy forms part of the information security/governance framework, which also includes the Information Security Policy, the IT code of Practice and the corporate Data protection policy.

Scope

- All users (employees, volunteers, contractors) wishing to use their smart mobile devices to gain access to Barnardo’s corporate IT network and use corporate applications.

- All groups and individuals identified as being responsible, for planning, implementing and maintaining the security of corporate data and corporate mobile devices.

- Outside of scope: Users wishing to continue to use the Barnardo’s guest network are excluded from this policy.

Definitions

- A smart mobile device is a tablet or smartphone capable of accessing the internet and running applications.

- The device may be owned by the user or owned by Barnardo’s. If owned by the user then it is termed a ‘Bring Your Own Device’ (BYOD). If owned by Barnardo’s then it is termed a ‘Corporately Owned, Personally Enabled device’ (COPE). In both cases the ‘device’ is able to be used by the user for both business and personal activities.

- A “device” is any smart mobile device that is authorised for connection to the Network.

- The Barnardo’s corporate IT network, the “Network”, is the means by which the device can provide users (employees, volunteers, contractors) with access to:

  a. Barnardo’s applications such as email.

  b. Barnardo’s information stored on systems such as Content Server and b-hive

  c. Barnardo’s data obtained from systems such as Service User Recording and Oracle.

- The Enterprise Mobility Management (EMM) system is an IT solution that allows secure management of smart mobile devices that connect to the Corporate Network.

- A ’jailbroken’ or ‘rooted’ device is one that has been tampered with to remove certain operating system limitations thus allowing it to bypass security features. As such, the device has been compromised and is not secure. It is not permitted to connect it to the Corporate Network.

Roles & Responsibilities

- Information Security Management is responsible for maintaining this policy and advising generally on information security controls.

- The IS Department is responsible for managing the security of corporate data and configuring security on authorised devices using EMM. IS is also explicitly responsible for ensuring the security of the EMM software and related procedures in order to minimise the risk of hackers exploiting EMM to access mobile devices.

- IS Service Desk will provide support for all devices and respond to calls regarding loss, theft and security breaches of any authorised devices.

- Authorising manager (i.e. budget holder) is responsible for granting COPE device access to the Barnardo's corporate network. They reserve the right to decline authorisation to any user, or to withdraw such authorisation, if they deem it inappropriate and not in the best interest of Barnardo's. BYOD access does not require approval.

- The user is responsible for:

  a. Following and complying with information security and data protection principles; especially unauthorised, unlawful processing or disclosure, accidental loss, damage or destruction of personal and organisational data.

  b. Reporting any security incidents affecting their device promptly to the IS service Desk in the normal way.

  c. To back up any personal information or data (e.g. pictures, mp3 files) should the device become corrupted or lost. Users should take care not to infringe other people's privacy rights, for example using devices to make unauthorised audio-visual recordings at work.

Authorisation and Acceptable Use

Only devices enrolled on Barnardo's Enterprise Mobility Management (EMM) solution will be allowed access to use the corporate IT network.

The Enterprise Mobility Management (EMM) solution configures and maintains a secure area (partition) on the device for accessing Barnardo's information and data. Any device that does not successfully pass the enrolment process will not be authorised for use.

Users may use their device to access the following Barnardo's owned resources: email, calendar, secure web browser and the Barnardo's Application store.

Users may use their device for personal use.

Devices not enrolled with EMM may connect to the designated guest network providing Internet connections, but will not be granted access to Barnardo's corporate IT network.

Information Security Management

1. Barnardo's maintains the right to control its corporate information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data on the device without reference to the user. Corporate data will be deleted if the device is compromised (e.g. stolen, lost), becomes non-compliant (e.g. jailbroken, rooted, unencrypted) or if corporate data is at risk.

2. Barnardo's recognises that users have a reasonable expectation of privacy over their personal information held on Devices, and have procedures in place to ensure that IS support staff do not have cause to access, or intentionally access, personal information.

3. Users shall take care not to infringe other people's privacy rights, for example only using Devices to make audio-visual recordings at work when authorised.

4. Users must take reasonable care to protect their device from loss or theft. If the Device is lost or stolen, the user must report the loss or theft to the IS Service Desk in the first instance and as a matter of urgency. In such an event Barnardo's shall use the EMM solution to "remotely wipe" all Barnardo's information on the Device.

5. Users use devices at their own risk. Users are advised to back up their personal information (e.g. pictures, mp3 files) such that it can be recovered in the event of corruption/ loss etc.

6. Barnardo's corporate information must be processed only in the secure partition on the Device.

7. Any Device which exceeds six weeks without establishing a connection with the EMM solution will have its enrolment revoked will be remotely wiped of all corporate data and the licence will be returned to the pool.

Devices and Support

Barnardo's will continue to provide its choices of managed computing devices as necessary for work purposes; there is no obligation for any user to opt-in to BYOD or COPE if they choose not to participate.

IS Service Desk will provide support for all Devices for EMM enrolment, connectivity, approved software selected by the business, and EMM system operational questions only. Given the multitude of different devices, BYOD devices will receive limited support on a 'reasonable endeavours' basis for business purposes only.

COPE Users:

- If a COPE device breaks or becomes damaged while conducting Barnardo's business, contact the IS Service Desk.
- Details of available COPE Devices can be found on b-hive.

BYOD users:

- The IS Service Desk will not support BYOD device replacement, device operating system upgrade, device operational questions or embedded software operational questions.

- If a BYOD device breaks or becomes damaged whilst conducting Barnardo's business, consult with your device's manufacturer or retailer for applicable warranty agreements or repair services. The user is responsible for notifying the IS Service Desk prior to sending their device for repair or replacing their BYOD device. On notification, Barnardo's will perform a remote wipe on the mobile device.

Financial

COPE devices and associated voice/data tariffs will be paid for by the IS Department who shall recover the cost from the requesting department. Whether the requesting department chooses to recover any of the cost from the user is between the requesting department and the user. Refer to b-hive for details of available COPE devices and tariffs.

Any reimbursement for voice and data charges incurred by BYOD users is a matter between the user and their department.

Associated guidance and documents

Guidance:

1. IT Security (including Information Security) and Data Protection training are available on b-hive.

Documents:

1. Information Security Policy
2. IT Code of Practice
3. Corporate Data Protection Policy

Document History

Version	Date	Author	Status	Comment
1	1st Sept 2014	Information Security Officer – IS Department	Definitive	Signed electronically by all users as part of sign-on.
2	31 Oct 2014	Internal Communications Manager – IS Department	Definitive	Adjustment to approval responsibilities.