Bring Your Own Device (BYOD), Offsite Working and Password Policy

Introduction

This policy applies to all people, including staff and volunteers who have access to The Brain Tumour Charity's systems and must be read in conjunction with our 'Access Policy' and 'Acceptable Use Policy'. Remote access to The Brain Tumour Charity's network, software and email system is provided to all staff and some volunteers, which is an essential component of our business continuity plan. The Brain Tumour Charity is committed to ensuring the safety of its employees, volunteers and assets and the protection of sensitive date. It takes the issue of physical and virtual security very seriously. This policy sets out the main precautions that must be taken and, together with the supporting documents listed, forms a significant part of our information security management.

Using your own device(s)

The Brain Tumour Charity encourages employees to use their own devices – PCs, tablets and/or smartphones and permits usage for the following activities:

Personal device:	Access email	Access network files via remote access	Store information	Develop information*
Desktop PCs and Laptops	Yes	Yes	Yes (via Desktop Sync)	Yes
Smartphones	Yes	Yes	No	Yes
Tablets	Yes	Yes	No	Yes

Employees using their own devices to access The Brain Tumour Charity's systems and data must adhere to the following:

- Implement a pin or password access to the device. This must comply with The Charity's Password Policy (see section below).
- Run Operating Systems that have not reached end of life support from their supplier and are still receiving regular patch updates, i.e. not Windows XP.
- Ensure that suitable anti-virus is installed and activated.
- Implement all anti-virus and/or system updates when prompted.
- Not use personal USB sticks or removable media cards (such as micro or mini SD cards) to store personal data or confidential information.
- Implement automatic screen lock after a period of inactivity.
- * Return information to The Charity's network as soon as possible once completed – to ensure that information remains accessible to those authorised to access it, and backed up.
- Avoid storing data locally i.e. use remote desktop, MS Teams etc. Where it is necessary to temporarily store data locally e.g. for off-line use, ensure it is deleted as soon as possible.
- Ensure The Charity's data and information is not accessible to any other people who may also use the personal device.
- **At all times everyone accessing Charity data and information must adhere to Data Governance, Protection and Retention policies.**

Offsite working

Employees are responsible for protecting The Charity's personal information and portable IT devices (e.g. laptops, smartphones, tables, removable media devices) against physical security threats, whether they are regionally based from home, office based and working from home or attending an external event. We will deploy an up-to-date anti-virus software to all employees working remotely. Employees must therefore ensure that each of their portable devices is connected to the network at least once every two weeks to enable the anti-virus software to be updated.

The following must be adhered to at all times:

- All users must ensure portable devices are kept in **separate locations** to the following at all times:
  - Access / authentication tokens
  - Passwords, personal identification numbers and/or codes.
- All users must only use removal media devices to store or share information in accordance with agreed procedures and/or protocols. See 'Sharing Personal Information Policy' and 'Access Policy'.

Portable devices

1. Portable devices should be locked away and kept out of sight when left unattended, and not left where it would attract the interests of the opportunist thief.
   - **At home**: personal data/screens should be located out of sight of the casual visitor, family members or others who share your accommodation. Charity owned devices should be put in a secure location, such as a lockable drawer when away for an extended period of time or fixed with a lock (e.g. Kensington lock).
   - **In transit:** not being left unattended for any period of time, including when visiting the toilet, buying refreshments, or otherwise being away from the information or device.
   - **At an event:** not left unattended and locked where possible to a desk/table. Any files containing personal data on the device must be password protected.
   - Be concealed when **being transported**.
2. Protected from unauthorised access when unattended, even for a few minutes, by:
   - Using the lock screen (<Ctrl> <Alt> <Delete> and selecting 'Lock Computer')
   - Locking the remote desktop (<Ctrl> <Alt> <End> and selecting 'Lock')
   - Switching them off
   - Logging off.
3. The Brain Tumour Charity provides some IT equipment that may be used in the office or offsite (at home or at an event) by office based staff. All equipment must be:
   - Signed out by the User taking the equipment, to acknowledge responsibility for its welfare.
   - Returned to the secure storage cabinet as soon as possible and signed in by the User.

Paper Records

Paper records containing personal data or confidential information (including notebooks), must be:

1. Locked away and kept out of sight when left unattended, and not left where it would attract the interests of the opportunist thief.
   - **At home**: located out of sight of the casual visitor, family members or others who share your accommodation.
   - **In transit:** Placed within a lockable unit (i.e. padlocked suitcase or cash tin) with the key held by a person travelling separately if possible, and not being left unattended for any period of time, including when visiting the toilet, buying refreshments, or otherwise being away from the information.
   - **At an event:** must not be left unattended or on display.
2. Concealed when being transported.

Password protecting electronic devices

Users must follow the Password Policy at all times and must follow the controls below at all times:

- Never reveal passwords or PIN numbers to anyone - including IT staff (at The Charity and any external IT providers) and their managers.
- Ensure passwords to The Charity's systems are not shared with others who share personal devices.
- Never use the 'remember password' function.
- Never write passwords or PIN numbers down or store them where they are open to theft.
- Never store passwords or PIN numbers in a computer system without encryption.

Strong passwords

All passwords must:

- Be a minimum of eight characters long.
- Include three of the following:
  - Uppercase character
  - Lowercase character
  - Number
  - Special character
- Not include proper names.
- Not include any part of the user's username.
- Not be the same or similar to any password used for non-work related activities.

IT responsibilities

IT (Development Team with Bluecube) will ensure the following measures are enforced by all Networks, System and Applications were possible. Any changes – i.e. due to the functionality of Systems or Applications – will be documented and the potential risk assessed by the Director of Finance and Governance before being implemented.

- Passwords must be changed every 90 days.
- At least the last four passwords cannot be re-used.
- The account will 'locked out' following four successive incorrect log-on attempts
- Password characters will be hidden by symbols.
- Ensure that log-on procedures are secure and do not provide unnecessary information.
- Be responsible for ensuring that secure authentication methods are used to access the IT network and security infrastructure, server and client operating systems and corporate systems such as internet and email.
- Ensure that new accounts are created with a temporary password which the user is required to change at first logon.
- Ensure that the initial password for an employee account will only be given to the new employee.
- Ensure that the login procedure is also protected by:
  - Passwords are not saved.
  - Limiting the number of unsuccessful attempts and locking the account if exceeded.
  - The password characters being hidden by symbols.
  - Displaying a general warning notice that only authorised employees are allowed.
  - Ensure a screen saver with password protection is enabled on all devices, and cannot be amended by employees.

Operating system access control apply to all computers and devices that have an operating system e.g. servers, PCs, laptops, tablets. See the 'Access Policy' for more information. System administration passwords are always available to a senior, nominated Officer, the Director of Finance and Governance, within The Charity who is separate to the System Administrator(s).

It is **essential** and a condition of employment that you password protect every device that you use to access Charity information/data, including any of your own personal devices - your smartphone, your iPad, your tablet, your home computer or laptop, your work laptop. For example, this may include accessing emails on your own iPhone, using the Cloud on your personal laptop, accessing Salesforce via your smartphone or outside of the Cloud on a home computer.

If you are accessing any system that holds data, i.e. the Remote Desktop, Egnyte, PeopleHR or Salesforce please **do not choose to remember the password**.

Any breach of this policy and rules may be considered Gross Misconduct or Negligence.

Version	1.2
Policy Owner	Pete Simmons
Last updated by	Pete Simmons
Last reviewed date	18/11/2020
Signed off by	Liam Heffernan
Signed off date	18/11/2020
Next review due	(Annual from sign off)