ACCESS POLICY

Last updated: March 2018 **Due for review: March 2019**

Updated by: Louise Taylor **Signed off by: Andrew Warren**

Introduction

This policy applies to all systems, people and processes that constitute The Charity's information systems, including staff, volunteers and suppliers who have access to The Brain Tumour Charity's systems. The Brain Tumour Charity is committed to ensuring the safety of its employees, volunteers, suppliers and assets and 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.

Physical security

The Brain Tumour Charity operates from one Head Office, based at Hartshead House, 61-65 Victoria Road, Farnborough GU14 7PA.

Physical entry controls

- The building is only accessed through one main door, which is monitored through CCTV. An alarm is activated outside of working hours when no key holders are present.
- The secondary door is an emergency access door only and can only be opened from within the building. This door is alarmed.
- All staff are issued with an access key fob. Door codes, which can overwrite the use of the key fob, are changed regularly and only shared with a limited number of key staff members.
- Limited, named staff are issued with a physical key, a log of which is maintained. Keys are restricted to staff who may be required to open or close the building or require access outside of normal office hours, e.g. events staff.
- Contracted cleaners are issued with a physical key to conduct their work outside of normal office hours. They undergo all necessary checks and are bound by the strict terms of their contract.
- All visitors to The Charity's premises, including volunteers, Trustees, contractors and suppliers, must:
    - Report to the reception area
    - Sign in to the visitor's book
    - Wear a visitor's/volunteer's/contractor's badge for identification
    - Sign out of the visitor's book on departure
- Visitors (excluding volunteers, Trustees and people under contract) must be escorted at all times whilst within non-public areas of The Charity.
- All deliveries must be made to reception. Individuals making deliveries or collections will only enter non-public areas whilst escorted by a member of staff. Any member of staff receiving deliveries of personal or confidential data will immediately move this to a secure location.
- Staff will challenge any unrecognised/unbadged person within non-public areas.

Equipment and paper security controls

- Limited information is stored in paper format in the offices. Any confidential information, including personal data, is held in locked cabinets. The keys for the locked cabinets are held in key safes.

- All equipment used to process and store personal information issued by The Charity is maintained by our IT providers in accordance with their contracts and may only be carried out with explicit agreement from the Development Department.
- No data is stored on servers in the office, these are all stored on servers in secure data warehousing facilities, managed through contracts with suppliers. The network equipment has UPS technology fitted.
- Network cabling is managed through an office system, which is locked and the key held in a key safe.
- Laptops for all staff use are held in a locked cabinet when not in use. The key for this is held in a key safe. All laptops are booked out and signed back in by individuals.
- Laptops issued to individual team members or meeting rooms are either taken home at night or, if left in the office, secured by Kensington Locks.
- No personal data is held on individual desktops, this is held securely either on our database or shared document storage system, which are encrypted.
- Standard removable media (i.e. USB sticks) must not be used to store or share personal or confidential data. If in extreme circumstances this is required, then an encrypted removable media device must be used, which can be borrowed from the Development Department and signed in/out by the individual.
- All screens must be locked when not in use.

Information security

This applies to all staff and volunteers at The Brain Tumour Charity 'users' who have been provided with access to The Charity's computer systems. Users are only provided with access to The Charity's network services that they have been specifically authorised to use. Access is managed by the Information Asset Owner based on business requirements as outlined below.

User access rights

Each user is allocated access rights and permissions to personal information and computer systems that:

- Are required for their role and the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Systems are established so that users are unable to override access controls.
- Where enabled by the security features of the software application, separation of duties and/or access into clearly defined roles is established.
- Logging functions i.e. to enable auditing and accountability of actions, are available only to administrators.

System administration accounts are only provided to users that are required to perform system administration tasks. The administrator account is not used by Systems Administrators for normal day-to-day activities.

Registering and deregistering users

All line managers must provide an employee set up form for every member of staff who starts, changes role or leaves The Charity. If volunteers require access to computer systems, a volunteer set up form must be provided. These forms are shared with nominated members of the team who have responsibility for registering and deregistering user access as follows:

System	Registration/Deregistration - Department	Access level
Network / remote desktop	Development	Access for all staff and limited volunteers. All unused accounts are deactivated. Temporary access can only be granted through the Development Team / VIP approval.
Office including Outlook	Development	Access for all staff and limited volunteers.

Salesforce CRM	Development	Access for all staff and limited volunteers. Access to data is based on role.
BRIAN	Research	Access only to the BRIAN databank staff team. No volunteer access.
PeopleHR	Core	Access to all staff. Access to data is based on role. No volunteer access.
PS Financials	Finance	Access only to the Finance team (full system). All staff have access to limited data via the portal. No volunteer access.
WorldPay	Finance	Access only to limited members of staff. No volunteer access.
Proposal Central	Research	Access only to limited members of staff. No volunteer access.
Eventbrite	Events	Access only to limited members of staff. No volunteer access.
Social media (Charity accounts)	Digital	Access only to limited members of staff. No volunteer access.
Social media (Charity groups)	Services and Influencing, Events	Access only to limited members of staff and volunteers.
Google Account	Digital	Access only to limited members of staff. No volunteer access.
Dotmailer	Digital	Access only to limited members of staff. No volunteer access.
Survey Monkey (main account)	Digital	Access only to limited members of staff. No volunteer access.
Survey Monkey (HR account)	HR	Access only to limited members of staff. No volunteer access.
Trello	Individual Teams	Access to all staff. No volunteer access. No personal data shared.
Facebook Workplace	Comms	Access to all staff. No volunteer access. No personal data shared.
Travel.CLOUD	Core	Access to all staff. No volunteer access. No personal data shared.
Sprout Social	Digital	Access only to limited members of staff. No volunteer access. No personal data shared.
SEMRush	Digital	Access only to limited members of staff. No volunteer access. No personal data shared.

Leavers

When a member of staff or volunteer leaves, all access is removed. Access to historic data (emails, My Documents) and rerouting of new emails is given to a nominated member of staff.

Third party access

Support for The Charity's IT systems, which can include personal data, is provided by third party suppliers. At all times, they will only act on instructions from The Charity as the Data Controller and remain bound by the terms of their contract, including confidentiality clauses.

Devices

The Charity's systems may be access through multiple devices, both Charity-owned and personal, as they are predominantly cloud based. How they should be used and protected is covered in the following policies:

- Acceptable Use Policy
- Offsite Working, Bring Your Own Device and Password Protection Policy.