ACCEPTABLE USE POLICY

Introduction

It is vitally important that we all take the protection of The Charity's data seriously, not only within the office but also at home and offsite. We have a responsibility to protect The Charity and the people we work for. This policy must be read and agreed in conjunction with all of our data protection policies.

All full and temporary employees and volunteers of The Charity must comply with this Policy when using The Charity's IT and personal information that The Charity is responsible for. From here on they are referred to as 'users.'

Anyone not employed by, or volunteering with, The Charity but using The Charity's IT is also subject to this policy and must comply with it. This requirement will be defined in all contracts.

Acceptable use

Email

The Brain Tumour Charity provides an email system to support business activities. Access to this system is granted to users on this basis.

All emails that represent aspects of The Brain Tumour Charity's business or administrative arrangements are the property of The Brain Tumour Charity and not of any individual employee and may be used, stored and accessed accordingly.

All external emails that are used to conduct or support our work must be sent using an **@thebraintumourcharity** address and contain the following information:

- Show the following details as a minimum for the sender: (i) Job title (ii) [Team / Directorate] (iii) Contact telephone number (iv) Email Address, to enable the sender to be identified.
- Include the following disclaimer which will be included in email signatures provided to all users by the Marketing and Communications Team:

  > Registered office: Fleet 27, Rye Close, Fleet, Hampshire GU51 2UH. Registered Charity in England and Wales (1150054) and Scotland (SC045081). This message (including any attachments) is intended solely for the person(s) to whom it is addressed (intended recipient). It may contain copyright, confidential and/or privileged information, within the meaning of applicable law. If you are not the intended recipient (or do not have authority to access the intended recipient's mail box) any disclosure, dissemination distribution or copying of this e-mail or any attached documents is strictly prohibited. If you are not the intended recipient please contact the sender as soon as possible and delete this e-mail and all attachments immediately.

  There may be instances where a user will receive unsolicited mass junk email or spam. Users should delete such messages without reading them and report them to Bluecube. Do not reply to the email or open any unknown attachments or click on links.

- Before giving your email address to a third party (e.g. via on online form or website) consider who the organisation is, and what controls that have in place to protect your email address. Consider the possible impact of your address being passed or sold to an unknown third party, and whether the benefits outweigh the potential problems.
- Chain letter emails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) must not be forwarded using The Brain Tumour Charity's systems or facilities.

Use of the internet

The Charity provides internet access to support business activities. Access is granted to The Charity's users on this basis.

Unsuitable use and unsuitable material

Please see ***Appendix A: Computer Misuse*** below for details of unsuitable use of the internet.

- Unsuitable material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other policies of The Charity.
- Accidental viewing of materials which infringes those mentioned above must be reported to HR.

Masquerade

It is an offence to masquerade as another employee on the internet and post articles in another person's name.

Participation in public internet forums and social media

The use of work related internet forums for professional or technical discussion is permitted.

- You must make every attempt to avoid bringing the name of The Charity into disrepute or to adversely affect its reputation, customer relations or public image.
- Non-work related services – such as social network sites, blogs, chat rooms and bulletin boards – must adhere to the above requirement.

Monitoring

At any time and without prior notice, The Charity maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems.

Whilst respecting the privacy of authorised Users, The Charity maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 to monitor and audit the use of The Charity's email systems and internet access to ensure adherence with this policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act and those Regulations, for example:

- Access will be necessary and proportionate, and must be carried out with due regard to the rights and freedoms of the employee (for example, their limited but permitted personal use).
- Managers must only open emails which are relevant to the business need in question.

Monitoring of content will only be carried out by staff specifically authorised for that purpose. These arrangements will be applied to all users and may include checking the contents of email messages, computers or removable media for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business.

Where a Manager suspects that the email and/or internet facilities are being abused by a user, they should contact the Talent team or if necessary the Director of Finance and Governance, the CEO or the Chair of the Governance and Ethics Committee. Staff in the Talent team are the only officers authorised to investigate and provide evidence and audit trails and authorise access to systems.
The Talent team will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Personal use

Limited, personal use of The Brain Tumour Charity's IT resources is permitted, subject to the restrictions contained in this policy and the other policies.

Personal use is defined as any activity that is not work-related or necessary in the performance of duties connected to the employee's employment.

Support must not be requested from other employees or Bluecube for personal use of IT resources.

Liability

- No personal use of The Brain Tumour Charity's IT can safely be considered entirely private and there should be no expectation of privacy. For example, there should be no expectation of privacy regarding personal emails sent from a work email account.
- The Brain Tumour Charity accepts no responsibility or liability whatsoever for any loss that an individual may suffer as a result of personal use of IT resources. This includes loss or disclosure of user personal information, and any loss or disclosure as a result of action taken to protect its IT, reduce business risks, protect its reputation or ensure legal compliance.
- Where requested and possible, user personal information held on The Brain Tumour Charity's IT resources will be returned to the user or authorised advocate. No liability for its loss or damage is accepted by The Charity either prior to, or during its transfer. The effort taken and method used to affect any such transfer will be reasonable and proportionate with any costs being borne by the user.
- Users using The Charity's IT systems do so at their own risk.
- In the event of loss or damage to software and/or hardware arising out of personal use recompense may be sought by The Charity.

Personal use of email

- Limited personal use of The Charity's email system is permitted, subject to the restrictions contained in this policy.
- Employees using The Charity's email system for personal mail do so at their own risk and The Charity accepts no responsibility for any disclosure of personal email messages or attached documents.
- Subscription to email mailing lists or list servers for personal purposes is not allowed, regardless of whether they are free or paid for services.

Personal use of the internet

- Limited personal use of The Charity's internet resources is permitted, subject to the restrictions contained in this policy.
- The playing of online computer games is not allowed.
- The Charity is not responsible for any personal transactions you enter into (for example, with regards the quality, delivery or loss of items ordered).
- You must accept responsibility for, and keep The Charity protected against, any claims, damages, losses or the like which might arise from your transaction (for example, with regards payment for items or any personal injury or damage to property they might cause).
- If you purchase personal goods or services via The Charity's internet service you are responsible for ensuring that the information you provide shows that the transactions are being entered into by you personally and not on behalf of The Charity.

Personal use of The Charity's IT devices

- Limited personal use of The Charity's IT devices is permitted, subject to the restrictions contained in this policy.
- They must not be used in relation to an external business.
- Only software supplied and approved by The Charity can be used.
- No family members may use the IT devices, they have been supplied for the employees' sole use.

Withdrawal of personal use

Personal use of The Charity's resources may be withdrawn at any time and without warning if:

- The use is considered inappropriate
- The use is considered an excessive use
- If any aspect of The Charity 's IT equipment, systems or networks are placed at risk
- If it is determined that any of the following restrictions have been breached; or
- It constitutes a breach of law.

Restrictions on personal use

The following further restrictions are placed upon all personal use:

- It must be reasonable, appropriate and not excessive
- It must not interfere with an individual's job responsibilities or those of any other employee
- It must not adversely impact or disrupt any other IT
- It must not harm, or be likely to harm, The Charity's reputation.

Further User Responsibilities

Users will:

- Not install or update any software or screensavers onto any Charity owned portable device.
- Not change the configuration of any Charity owned portable device.
- Not install any hardware to or inside any Charity owned portable device, unless authorised by Development.
- Allow and facilitate the installation and maintenance of Charity owned installed anti-virus updates immediately.
- Inform the Development Team of any Charity owned portable device message relating to configuration changes, and report any faults immediately.
- Not remove or deface any asset registration number.
- Fully co-operate with any audit of software and hardware, which may occur without notice and require the removal of any device for further inspection.
- All Charity owned devices must be returned to the Development Team for secure disposal or reissue when no longer required.

Loss or theft of electronic devices

If at any time you lose a device that has access to our data, including any personal devices, please inform the Development Team immediately, so we can reset passwords for all accounts.

Adherence to policies and procedures

All Users must also adhere to The Brain Tumour Charity's:

- Bring Your Own Device(BYOD), Offsite Working and Password Policy
- Access Policy
- Data Protection Policy
- Data Governance Policy
- All other policies, procedures and guidance as required by their role at The Charity.

The Charity considers any breach of these rules to be gross misconduct for which the normal sanction will be summary dismissal.

Version	1.1
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)

Acceptable Use Policy Appendix A: Computer Misuse

There is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for the pursuance of personal interests or for amusement/entertainment. The purpose of this policy is to establish guidelines as to what constitutes 'computer resources' what is considered to be 'misuse'. This policy should be applied whenever Users who access information systems or information utilise The Charity's computer resources.

The misuse of The Charity's computer resources is considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action including dismissal.

Computer resources include, but are not restricted to, the *following*:

• Desktop computers	• Tablets	• Smartphones
• Laptops	• Printers	• Network equipment

This appendix to the Acceptable Use Policy does not define an exhaustive list all possible forms of misuse of computer resources; individual circumstances of each case must be taken into account.

In general, Users will:

- Comply with the Data Protection Policy and Supporting Polices and its associated guidance, and will comply with the Computer Misuse Act 1990.
- Not attempt to use computer systems to gain unauthorised access to information and software, or to cause system outages.
- Not deliberately introduce malicious software – such as computer viruses – onto The Charity's network infrastructure and information processing systems.
- Take all reasonable steps to prevent the transmission of viruses – by making full use of The Charity's anti-virus software, ensuring it is operating on any device they are using.

Use of the internet and email must not infringe the general principles of use which are set out below:

- Defamatory material, and material of a libellous or obscene nature, must not be created, published, posted or communicated, whether internally or externally.
- Any website or email that is perceived to be potentially offensive to anyone must not be viewed or transmitted. This will include material that:
  - Discriminates, or encourages discrimination, i.e. age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex, sexual orientation.
  - Is designed or likely to cause annoyance, inconvenience or needless anxiety, or otherwise abusive or threatening to others, or serves to harass or bully others.
  - Is offensive, obscene or an indecent image, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
  - Please note, the material listed is neither exclusive nor exhaustive.
- Material that infringes the copyright of another person, including intellectual property rights, must not be published, posted or communicated, whether internally or externally.

Some further examples of misuse are outlined below:

- Use of computer resources for the purposes of fraud, theft, dishonesty, hacking or other cyber-crime.
- Use of computer resources to corrupt, destroy or disrupt the data of other users or breach their privacy.
- Storing/loading/executing of software for a purpose which is not work related.
- Storing/loading/executing of software:
  - Which has not been acquired through The Charity's procurement procedures, or
  - For which The Charity does not hold a valid program licence, or

    - Which has not been the subject of formal virus checking procedures.
- Wilfully or deliberately jeopardising the integrity or function of any IT – e.g. transmitting by email any file attachments which they know to be infected with a virus; downloading data or programs of any nature from unknown sources; forwarding virus warnings to other users (other than to IT).
- Breaching the Access Control Policy or the BYOD, Offsite Working and Password Policy.
- Unauthorised disposal of IT – for example, destruction, removal or scrapping.
- Theft of IT or any parts of any IT equipment.