Brigitte Trust

E-Safety Policy

1 Introduction

The use of Information Technology including Telecommunications (ITC) provides excellent opportunities that can benefit Brigitte Trust and its clients. However, these technologies, if not used appropriately and safely, can represent significant additional risks.

The policy relates to all ITC facilities and services of the Trust.

This policy is to provide the good practice guidance and rules which staff and volunteers working for the organisation shall follow when using IT equipment, accessing the internet and using e-mail and other electronic methods of communication. It covers working in the office, working whilst in the community and remotely accessing Brigitte Trust's files and/or e-mail.

It is essential that all employees and volunteers adhere to the policy. Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include reporting to the police, dismissal and/or the offender being denied access to the Trust's ITC facilities.

2 Aims

The safe and efficient use of all forms of ITC, including that:

- Data are held securely
- Communications of confidential data are secure
- Files can be shared efficiently with authorised levels of access
- Employees, volunteers and those we support or are in contact with are protected from abuse.

3 Brigitte Trust's Property

All Brigitte Trust's ITC facilities and information resources remain the property of Brigitte Trust and not of particular individuals, teams or departments. By following this policy we will help ensure ITC facilities are used legally, securely and effectively.

4 Copyright & Software Licensing

The Internet and e-mail may contain data that are under copyright or software licence. Both the downloading and onward transmission of such material may constitute copyright infringement.

- Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements
- Do not breach copyright or other legal limitation on the use of published data or images by ensuring that the owner of such material allows this or there is a licence to do so
- Use of software or other material outside these agreements is illegal and may result in criminal charges

5 Security

5.1 As an employee or volunteer, you must not:

- Attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents
- Install or download any unauthorised software. Do not delete or modify in any way software that has been installed on your computer. If you do not have access to the information resources or software programme you feel you need, contact the Charity Administrator
- Disclose personal system passwords or other security details to other employees, volunteers or external agents, and do not use anyone else's login except with the written permission of the Chief Executive. If someone else gets to know your password, ensure you change it immediately
- Store confidential or identifying material on portable data storage devices for use outside of the Brigitte Trust office. If using a portable data storage device then it must be password protected
- Open e-mail unless you have a reasonably good expectation of what it contains, e.g. don't open "explore.zip" sent from an address you have never heard of, however tempting. This is one of the most effective means of protecting Brigitte Trust against e-mail virus attacks.

5.2 If you leave your PC or laptop unattended ensure it is locked or that you are logged off. You are responsible for any misuse of it while you're away. Do not leave a laptop in view in an unattended car or other vehicle.

5.3 Always check disks and other portable data storage devices for viruses, even if you think they are clean. Computer viruses are capable of destroying Brigitte Trust's information resources. It is better to be safe than sorry. Please seek advice from your Line Manager if you need help.

6 Data Protection

The use of the Internet and E-mail is covered in the Data Protection Act 1998 (DPA). If you are recording or obtaining information about individuals, be sure you are not breaking Data Protection legislation. Only record information with an individual's permission and only that information that is necessary to provide a safe and efficient service.

The eight UK data protection principles set out below, which relate to personal data, are recommended as a guideline; these state that data shall be:

- Fairly and lawfully processed
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure

- Not transferred to other countries without adequate protection

Ask your Line Manager if you are in any doubt about the relevance of recording and storing any information.

7 Public Image

You are a representative of Brigitte Trust when you are on the Internet using e-mail or other electronic means of communication.

- Do not make comments that may bring the organisation into disrepute
- Do not make defamatory statements about Brigitte Trust, its clients, employees or volunteers or any other person in any communications including those posted on any social networking site e.g. Facebook or Twitter
- Make sure your actions are in the interest and ethos of Brigitte Trust and do not leave Brigitte Trust open to legal action (e.g. libel)
- Avoid trading insults with other people using the Internet with whom you disagree
- The same laws apply to electronic communication as to any other written document.

8 Obscenities/Pornography

The downloading of offensive, obscene or indecent material to Brigitte Trust ITC facilities is forbidden. Employees and volunteers should be aware that the downloading or transmission of certain images is a criminal offence and that, in addition to its internal disciplinary procedures, Brigitte Trust may inform the Police where there is any evidence of such an activity.

Do not write it, publish it, look for it, bookmark it, access it or download it.

9 Electronic monitoring

Any information available within ITC facilities must not be used to monitor the activity of individual employees or volunteers in any way e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their e-mail or private files etc.

The exceptions to this policy are:

- In the case of a specific allegation of misconduct, when the Charity Manager or Chair of Trustees can authorise accessing of such information when investigating the allegation
- When the IT support personnel cannot avoid accessing such information whilst fixing a problem
- If an employee or volunteer is absent from work for an extended period of time or is on holiday and it becomes necessary for the Charity Manager or Chairman to authorise access in their absence
- When an employee or volunteer leaves Brigitte Trust it is necessary to check and open e-mails that may be sent to them after they have left.

In such instances the person concerned, if still in employment with the Trust, will be informed immediately and information accessed will not be disclosed wider than is absolutely necessary.

In the case of alleged misconduct an employee's or volunteer's access to IT facilities may be disabled pending investigation.

10 E-Mail

10.1 When to use e-mail

- Use e-mail in preference to paper to reach people quickly and to save time on printing, copying, distribution and to help reduce paper use. Check messages before sending as you would a letter
- Use the telephone for urgent messages, including voicemail if no reply, backed up where appropriate with e-mail
- Note that e-mail is not a totally secure medium and therefore it must not be used for transmission of confidential information, including information identifying employees, volunteers or those we support. Attachments containing confidential information must be protected with a password which is passed to the recipient in a separate e-mail or verbally
- The requirements of the Data Protection Act must also be observed when personal information is included in e-mail.

10.2 Use of Distribution Lists

- Only send an e-mail to those it is meant for; do not broadcast unless absolutely necessary since this runs the risk of being disruptive. Unnecessary or junk e-mail reduces computer performance and wastes disc space
- If in any doubt about whether individuals on an e-mail distribution list have given their permission for their contact details to be shared, then a group e-mail should be sent using the "blind copy" (bcc) facility
- If you wish to broadcast non-work related information or requests e.g. information or opinions on political matters outside the scope of Brigitte Trust's campaigning, social matters, and personal requests for information etc. then use a webmail account or a personal e-mail account at home.

10.3 General points on e-mail use

- When publishing or transmitting information externally be aware that you are representing Brigitte Trust and you could be seen as speaking on behalf of the organisation. Make it clear when opinions are personal. If in doubt, consult your Line Manager
- Check your inbox at regular intervals during the working day and keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each e-mail as you read it e.g. delete it, reply to it,

mark it for follow up, save the e-mail in a folder, or extract just the useful information and save it

- Keep electronic files of electronic correspondence, only keeping what you need to. Do not print it off and keep paper files unless absolutely necessary
- When sending e-mails:
    - Make clear the purpose or expected outcome e.g. “for information”, “for action”, “urgent” etc. Using accepted prefixes e.g. FYI will help recipients deal with mail efficiently
    - Treat others with respect and in a way you would expect to be treated yourself e.g. do not send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions or decisions of a colleague
- Do not forward e-mails warning about viruses as they are invariably hoaxes
- External e-mails must include the Charity’s disclaimer statement, name, charity and limited company registration numbers. Copy can be got from the Brigitte Trust website staff area.

10.4 E-mail etiquette

- Be courteous, it is more likely to get you the response you want
- Do address someone by name at the beginning of the message, especially if you are also copying another group of people
- Always insert a clear, relevant subject header e.g. Do not use subject headers like "stuff", remembering that the recipient may use the title to access it again in the future
- Try to keep to one subject per e-mail, especially if the content is complex. It is better for your reader(s) to have several e-mails on individual issues, which also makes them easy to file and retrieve later. One e-mail covering a large variety of issues is likely to be misunderstood or ignored
- Avoid using capitals, bold or underlining e.g. to emphasise words, as it commonly perceived as 'shouting'
- Keep e-mail signatures short. Your name, title, phone and web site address may constitute a typical signature.

11 Storage of E-Information

- All documents that are created on the computer or that have been received as attachments via an e-mail must be saved in the appropriate place
- No documents must be saved to either the “Desktop” or to the PC or laptop hard drive i.e. not to “My Documents”
- All documents must be saved to the appropriate folders on the Network Drives
- Information stored by Brigitte Trust may be subject to the provisions set out in the Freedom of Information Act 2000 and as such it is critical that documents are stored correctly and for the appropriate length of time.

If you are unsure of how to store electronic documents please talk to Administration.

12 Remote Access to IT, Internet and Data

- Subject to being given appropriate authority, employees or volunteers may have remote access to the Brigitte Trust server and internet systems. The need for remote access will be determined by the nature of the work and with the authorisation of the Charity Manager.
- Before remote IT access is allowed, employees or volunteers must sign an undertaking agreeing to follow the guidance and rules set out in this E- Safety policy, other relevant policies, and specific instructions relating to their area of work. The undertaking will be returned to Administration and retained in the individual's personnel file.

- Line Managers are responsible for ensuring that access is cancelled at either the end of a project, during a period of extended absence or when the employee or volunteer leaves the Trust. This will be done by dating and countersigning the original authorisation form and passing to the IT Administrator to block future access.
- Employees or volunteers who are issued with portable IT equipment are responsible for its care and safe-keeping. They must ensure that it is kept in a safe place at all times and that it is within their control. Under no circumstances must it be lent, used or left in the care of non-Brigitte Trust personnel.
- When connecting to the Brigitte Trust internet or e-mail system, or remotely accessing the Trust's data files, employees or volunteers:
  - Are responsible for ensuring there is no possibility of being overlooked and thereby causing a breach of confidentiality. Please take extra care when working in public places.
  - Must under no circumstances use tick boxes (e.g. remember me sign-in or log-in giving the history of their password) when signing in on any computer, laptop, mobile phone or other device in the office or in accessing remotely
  - Must terminate fully any session of remote access immediately when the session is complete by logging off.
- Authorised employees or volunteers may be able to access files from another organisation's premises. Files that are accessed in these circumstances must not be copied or moved onto the other organisation's server or network drive without the written permission of the Charity Manager
- Files should not be altered or amended without prior authorisation from either the creator of the file or Line Manager. The "Track Changes" facility should be used to clearly identify contributors to a document or file
- If a client file is accessed and added to or amended by an employee or volunteer, they must add their name to the change or addition.

13 Personal Use of Internet and E-Mail

Brigitte Trust does not encourage the private use of the internet or sending of private e-mails from the Trust's facilities. Such use should be strictly limited and should follow the same principles and guidelines set out in this policy for using the internet at work. Under no circumstances should:

- Your work e-mail address be given out as a personal contact for non-work related activities
- Any personal documents be saved on any Brigitte Trust computers or network.

14 Mobile Phones

The Trust recognises that staff may need to be contacted by family members, or school during work hours and that personal mobile phones need to be accessible during work time.

However it requests that staff do not use their personal mobile phones to make or receive unnecessary calls during work hours, nor to access the internet for personal use via their phones in work hours.

Date reviewed	December 2019
Date to be reviewed	December 2022
Date approved	February 2020