PARKHAVEN TRUST

Information Technology and Data Security Policy: IG02

Contents

1. Introduction

Information Technology (IT) is an integral and critical part of Parkhaven Trust's business and will have a significant impact on the efficiency of Parkhaven Trust. Parkhaven Trust takes steps to maintain the integrity of its systems and protect itself from risk associated with loss of information due to hardware failure or attack by computer viruses. Parkhaven Trust seeks to ensure the responsible and ethical use of IT in providing efficient and effective communication and good management and to minimise waste by reducing paper usage.

This policy should be read in conjunction with the Data Management policy.

The term 'user' refers to any employee, volunteer or Trustee who accesses the Parkhaven Trust network via computer, email account, laptop, tablet, smartphone or other mobile device.

2. Access to Data

Users can access Parkhaven Trust data via a number of methods: smart phones, tablets, laptops, handsets, thin client and PC's

Smart phones, tablets & Laptops
If a device is provided to assist an employee in doing their job it must not be used for personal matters without permission. For a member of staff to obtain authorised and secure smart phone access to our data and be issued with the required mobile device, their relevant Line Manager should ensure the user complete a mobile device assignment form. See appendix 1.

Managers should not just transfer phones from one staff to another but return the device to the administrator. Technical problems or queries regarding remote access or mobile devices should be addressed to the Parkhaven Trust Administrator. Users must return all smart phones to the administrator when access is no longer required, or when leaving the organisation. All data from returned devices should be deleted or archived and the device reset and wiped.

All mobile devices issued will be installed with appropriate and approved encryption & PIN control. All Trust laptops are encrypted and any laptops used for remote working will be set up with VPN's and 2 factor authentication.

All devices should be held and transported securely, should not be left unattended (e.g. in vehicles), and should be locked away when not in use. Users must not install any unauthorised or unlicensed software on any Parkhaven Trust issued device. Issued mobile devices should not be used for non-business-related purposes and must only be used by the individual that they have been issued to. A user may not share the device with or lend it to anyone else, for example a family member or work colleague. Stolen or lost equipment must be reported as soon as possible to the Parkhaven Trust Administrator and the Finance and Information Manager

Users are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems. Device screens should be locked when not actively being used. The use of devices in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of equipment. Staff must ensure

that Parkhaven Trust's devices and information accessed at home are secure from theft and damage and cannot be accessed by family members, friends or any other unauthorised user. Data should not be held on a device for longer than it is required and should be deleted or archived promptly to reduce the risk of the data being accessed by the wrong person. Personal confidential data must not be stored on an unencrypted device (***NB: Password protection is not a method of encryption and must not be relied upon as such).***

Personal devices

Users will not use personal devices to access our services or data except for email access and then only when the device has been risk assessed by Parkhaven Trust's IT provider and permission granted All documents will be accessed via email only and not saved elsewhere, including the device itself or the cloud / external media devices. Email access must be via the nominated device only. In the event that an approved device is lost or stolen, or is suspected of having been lost or stolen, the company must be informed as soon as possible so that such steps as may be appropriate may be taken to delete from the device the companies email account. Approved anti-virus software must be used on approved devices and must be kept up to date. The latest security updates to the operating system and browser software must be routinely installed on approved devices (this does not require the installation of an entirely new version of the operating system). Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure. If an approved device needs to be repaired, appropriate steps must be taken to ensure that confidential information cannot be seen or copied by the repairer. In the event that an approved device needs to be disposed of please contact Parkhaven Trust so that the appropriate steps can be taken to remove the email account from the device. In the event a user leaves the company, appropriate steps must be taken to the satisfaction of IT services to remove the company email account and other data belonging to the company, from approved devices. The date on which those steps are taken and the date on which those steps are approved by IT services must be recorded in the list of approved devices.

Mobile care planning devices

The use of electronic care planning has reduced the amount of paperwork for all staff across Parkhaven Trust, enabling Parkhaven Trust to share information much more effectively, and provide accurate information to outside agencies.

The mobile care monitoring system holds all of the personal information relating to a service user. Accessing the mobile care planning system via a handset enables the user to view all of the personal information for all of our service users whilst on the move. The handsets must not be left anywhere unattended or shared with other members of staff. All handsets are numbered and must be allocated to a member of staff at the beginning of each shift. A record must be kept who the handset was logged out to at what time and when it was returned. If a handset is not returned at the end of the shift the shift leader is responsible for contacting the member of staff who was allocated the handset to find out why the handset has not been returned and to arrange for the handset to be returned immediately. The shift leader must immediately disable any handsets that are not returned. A member of the public gaining access to the handset is a serious data protection breach. Therefore all lost handsets must be disabled immediately and reported to the service manager to ensure this information is not accessible by anyone outside of Parkhaven Trust

A handset that is not returned and not immediately disabled results in a data protection breach which must be reported to the Finance & Information manager. If a handset breaks this must be logged by the shift leader and reported to the service manager.

Thin clients & PC's

Within Parkhaven Trust buildings users access the network either via thin clients or PC's. Both are password protected. A user cannot access the network without a user name and password supplied by the administrator. Users must not share their username and password. All users must log out of the system at the end of each day or if they leave their desk for a period of time. Extra care should be taken if food or drinks are consumed close to computer equipment. An enforced disconnect after 30 minutes idle is in place.

3. User Access control

When setting up a new user access a user risk assessment will be undertaken to determine the security requirements given the data concerned. For example, the level and type of access controls, location of hardware associated with the system, type of data held, etc.

The File storage systems have been constructed in order to ensure all and only appropriate personnel have access to a folder which can then be viewed, altered, copied or deleted. The HR systems and the electronic care planning system haven been set up with different levels of access according to job role.

New accounts must then be requested by managers using the 'IT *new starter form*' (appendix 2) and sending the form to the IT administrator providing the relevant information. The IT administrator is responsible for the creation and deletion of accounts, permissions and password resets on Parkhaven Trusts network. For the other systems used by Parkhaven Trust the information asset owner is responsible for additions, amendments and deletions. The IT form must be sent to the necessary information asset owner by the IT administrator.

User accounts must be amended immediately upon there being a change in the staff team to ensure that all user accounts are appropriate. This includes creation and removal of access rights. Amendments or deletion of accounts is requested by the manager using an 'IT leaver /change form' (appendix 3) which is sent to the IT Administrator who will forward it to the relevant information asset owner if required.

4. Data Security

Parkhaven Trust uses the services of an external provider to maintain and advise on the security of the IT system

Security of Manual Records

To prevent the accidental loss, destruction or disclosure of personal or sensitive data held in employee or service user records, paper records will be secured as follows.

Line managers may only have access to personnel files for employees they either directly manage or their subordinates manage, or to files for service user to whom they directly provide care.

Line managers will ensure that all employee and service user files are locked away securely when not in use and at the end of the day. It is good practice to maintain a 'clean desk' policy and this should be a part of the above practices.

Security of Electronic Records
Managers may hold sensitive and personal service user data on the computer. In such instances the same access and security protocols will apply as for employee records. The computer system will operate an automatic log out after 30 minutes.

Parkhaven Trust has a cloud based Human Resource system which contains sensitive information on employees and a cloud based system for electronic care planning in the majority of its services.

To prevent the accidental loss, destruction or disclosure of personal or sensitive data held on computer records will be secured as follows.

- Line managers may only have access to data files that they either directly manage or their subordinates manage.

- Access will be controlled as above and will be password protected. Employees must follow the password protocols below.

Identity theft
Users must be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees must:

- ensure that no information is made available that could provide a person with unauthorised access to Parkhaven Trust and/or any confidential information; and
- refrain from posting any confidential information regarding Parkhaven Trust on any social networking website

Software & Storage Media
Users must not bring any software or storage media (e.g.: USB memory stick) on to Parkhaven Trust's premises. If data needs to be transferred to or from Parkhaven Trust's computer system for any reason, permission must be obtained from the IT Administrator prior to the transfer and the storage media must first be virus-checked. Users may only use software provided by Parkhaven Trust. Users must not put any software on the computer system or mobile devices or copy any software provided by Parkhaven Trust. Users must not remove any storage media, documents, software, data or other information or materials from Parkhaven Trust's premises without prior authority.

Users must not cause a computer to perform any function with the aim of obtaining unauthorised access to any software or data. Users are warned that a breach of this rule could also be a criminal offence under the Computer Misuse Act 1990. Users are only permitted to use the system and have access to information that is relevant to their job. Users should neither seek information nor use systems outside of this criterion unless specifically authorised to do so by their line manager.

Public cloud-based sharing and public backup services, should never be used for the storage any Trust data without the express permission of the Finance & Information Manager.

Users must not perform actions or use software that may affect the security of Parkhaven Trust's computers or its software.

All information stored on the computer remains the property of Parkhaven Trust.

Password Management

Passwords are confidential information and must be treated as such. Users must not disclose their passwords to anyone. Each user is responsible for maintaining the security of their individual login and password. If a breach of security is recorded under a user's login the burden of proof will be placed on that user to show they are not responsible for the breach. Passwords must be at least 12 characters long, be a mixture of at least 3 of the following: upper case letters, lower case letters, digits and symbols and easily remembered so there is no need to write it down.

Passwords must not be automatically saved on devices. If a user becomes aware of another user's password they must inform that user immediately.

Printing

When printing only print the minimum amount of data needed: ensure that you are near the printer to be able to pick it up immediately. Store the printed information securely until you can dispose of it securely.

5. Email

Parkhaven Trust's email system is intended primarily for business use. Users are permitted to use email on a limited basis for personal reasons but personal advertising is not permitted under any circumstances. Users must not send personal emails during their normal hours of work.

When sending emails users must use the Parkhaven server and not remote/internet email facilities. The sending of emails via remote sites or using another user's login to send emails will be considered gross misconduct.

All messages must be sent using Parkhaven Trust's standard template so that the signature, disclaimer and other standard details appear.

Parkhaven Trust reserves the right to access emails at any time. Even when an email has been deleted, it can still be retrieved from the back-up system and therefore privacy cannot be guaranteed. Parkhaven Trust reserves the right to monitor emails (in accordance with data protection legislation). Users have the right to object to processing of this nature, Parkhaven Trust will consider such objections on a case-by-case basis and provide a full explanation for their decisions.

Confidential or sensitive information may not be fully secure when sent via email. Attachments containing multiple personal records or any sensitive / special category personal information must be encrypted in transit and must only be sent to authorised recipients. Think carefully before forwarding such information to anyone.

Email messages are only to be accessed by the intended recipient.

All messages composed, sent, received and stored on the email system remain the property of Parkhaven Trust. Parkhaven Trust owns the copyright of all material created by employees for use on the email system.

Users must check their business email messages regularly. If a user is unable to access their email account for a significant period e.g. holiday, it is their responsibility to ensure that an 'out of office' message is set up on their email account with details of an alternative contact should the message be urgent.

Users must be mindful that emails sent on behalf of Parkhaven Trust must be drafted in a professional manner.

Messages sent via the email system could give rise to legal action against the sender and/or Parkhaven Trust. Claims of defamation, discrimination, breach of confidentiality or contract could arise from misuse of the system. It is therefore vital for email messages to be treated like any other form of correspondence and, where necessary, hard copies to be retained. Users are reminded that messages may have to be disclosed in Court or Tribunal proceedings.

An email message must not contain material that could be construed either by the recipient or by a third party as abusive, discriminatory, obscene, offensive, defamatory or insulting. In this respect users should bear in mind that so called "joke" emails can very easily fall into any of these categories. Inappropriate statements regarding customers, competitors or suppliers and their products / services are also prohibited. Both the individual user and Parkhaven Trust may be liable for any such material being sent. If a user receives a message that contains such material, they must not forward it to anyone else and must notify their manager immediately.

The amount of email in a user's inbox must be kept to a minimum. Non-essential work emails should be deleted after reading. Saved emails must be reviewed on a monthly basis and deleted when no longer required. It is good practice to move emails that need to be saved to a personal folder. Care must be taken when sending file attachments as these are typically large and may cause congestion. File attachments must only be sent when necessary and deleted as soon as possible. The same housekeeping rules apply to sent items. Users are responsible for their own housekeeping. The size of email accounts will be monitored.

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Users must not use Parkhaven Trusts resources to distribute spam emails. Junk mail is usually a result of spamming. Parkhaven Trust is striving to improve its Junk mail detection but unfortunately no system is 100%. Users must be vigilant when opening emails.

Computer viruses, Trojan horses and worms are collectively known as malware. The most common method of distribution malware is via email. Users should not open emails or click on any hyperlinks from an unknown source. Furthermore, under no circumstances must users open zip files within emails or download any application. If a user is in any doubt please contact the IT provider immediately.

6. Internet usage

Parkhaven Trust's internet account is intended primarily for business use. Users must obtain permission from their manager before using the internet for personal reasons. Permission may be refused for any reason and access may be subject to certain conditions, Parkhaven Trust does not allow access to social networking websites or webmail from its computers. If users access the internet for personal reasons, this

should take place outside their normal hours of work or during their agreed breaks from work.

Parkhaven Trust reserves the right to add websites to the list of restricted websites without notice or consultation with users.

Users must not access websites containing any pornographic or other offensive material or download any such material. Users must not download to Parkhaven Trust's network any software, games, screensavers or similar items from the Internet (either directly or by transfer from storage media), unless approved by Parkhaven Trust and subjected to virus-testing procedures. As well as the possibility of viruses, others may have copyright in this material and, if it is downloaded it could lead to legal action being taken against Parkhaven Trust.

If a user feels that they have accidentally accessed an inappropriate internet site this should be reported to their line manager and Parkhaven Trust Administrator as soon as possible. Users have a responsibility to report any security incidents or suspected incidents.

Users must obtain permission from their manager before putting any material on the internet. This is because someone else may own the copyright to this material. This could result in unauthorised downloading, leading to a claim against Parkhaven Trust. Parkhaven Trust owns the copyright to all material created by employees for use on the internet.

Users must be careful that they do not make unauthorised use of the trademarks of others on the internet and should watch out for the unauthorised use of Parkhaven Trust's trademarks by others.

Users must not place any defamatory, discriminatory, obscene or confidential material on the internet.

Parkhaven Trust reserves the right to monitor users' internet usage, but will endeavour to inform an affected user when this is to happen and the reasons for it. The privacy of any messages or information (in whatever form) sent or received by users on the internet cannot be guaranteed. Users have the right to object to this monitoring and Parkhaven Trust will consider such objections on a case-by-case basis and provide a full explanation for their decisions. Parkhaven Trust considers that valid reasons for checking a user's internet usage include suspicions that the employee has:

- been spending an excessive amount of time viewing websites that are not work-related; or
- acted in a way that damages the reputation of Parkhaven Trust and/or breaches commercial confidentiality, or
- been engaged in activities which could amount to a breach of trust and confidence between the user and Parkhaven Trust.

7. Social Media

Parkhaven Trust recognises that many staff participate in social networking on websites such as Facebook, Twitter, etc.

Parkhaven Trust has a Marketing & Fundraising manager who is the owner of the Parkhaven Trust social media sites and is responsible for any engagement through these sites and for responding to customer enquiries. Employees must not attempt to respond to enquiries or comments directed specifically at the company or asking for a company response. Any information posted on social media by Parkhaven Trust can be shared by all users.

Parkhaven Trust respects staffs right to a private life. However, a member of staff who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual or Parkhaven Trust. Parkhaven Trust must also ensure that confidentiality and its reputation are protected and that staff do not expose Parkhaven Trust to potential liabilities. It therefore requires staff using social networking websites to:

- refrain from identifying themselves as working for Parkhaven Trust;
- ensure that they do not conduct themselves in a way that is detrimental to the employer
- take care not to allow their interaction on these websites to damage working relationships between members of staff and service users of Parkhaven Trust.
- refrain from posting any images of staff or service users or any images taken in the workplace, on any aspect of social media
- refrain from using social media to bully another individual such as a co worker
- refrain from posting images that are offensive
- refrain from breaching any confidentiality or other relevant policy

Users should be aware that social networking websites are a public forum, particularly if the user is part of a "network". Users should not assume that their entries on any social media site will remain private and are reminded that social media is never completely private, everything is in the public domain so there is no reasonable expectation of privacy. Staff should never send abusive or defamatory messages.

8. IT Admin access

All data and systems can be accessed by the IT system administrators (in accordance with relevant procedures). Please ensure that anything you store on Trust systems is related to Trust work. In the event you store a personal file this would be accessible to the system administrators. This is particularly relevant if there is a GDPR related request.

9. IT Training

GDPR, Information Governance and Cyber Security training is part of the induction programme and mandatory training for all staff and volunteers.

10. Business Continuity

Parkhaven Trust is aware that some form of disaster may occur resulting in IT failure. The manager of each service will create and maintain a file, containing paper copies of all forms which they use on a day-to-day basis. In the event of an IT failure this file will enable managers to create copies of essential documents and minimise the impact of

the IT failure. All information held on the network is backed up every night. All information held on the cloud via service providers is backed up continuously.

11. Other Information

Any breach of this policy will constitute misconduct which is likely to lead to disciplinary action being taken against the offending employee. Depending on the nature of any breach and the consequences to Parkhaven Trust, this may be regarded as gross misconduct and lead to dismissal without notice or pay in lieu of notice and potentially legal action.

Finance & Information Manager
November 2024

Appendix 1

<table>
<tr><th colspan="3">Parkhaven Trust Portable Device Assignment Form</th></tr>
<tr><td colspan="2">Type of asset [tick]:
Laptop
Mobile phone
Memory stick
External hard drive
Tablet
Other [insert type] ……</td><td>Make and model:</td></tr>
<tr><td colspan="2">If the asset is a mobile phone, enter number:</td><td>Serial number:</td></tr>
<tr><td>Date entered on information asset register:</td><td>Equipment is encrypted: [circle]
YES NO N/A</td><td>Indelibly marked to indicate the property of the organisation: [circle]
YES NO</td></tr>
<tr><th colspan="3">STAFF INFORMATION</th></tr>
<tr><td colspan="3">Allocated to:
Job role:</td></tr>
<tr><td colspan="3">STAFF DECLARATION
I, [print name] …….. understand and agree to comply with the Parkhaven Trust staff guidelines on using mobile computing devices and related procedures as outlined in the Data Protection Policy and associated policies.
I understand that:
• It is my responsibility to report immediately any theft, loss, damage or misuse of the above asset using the Data Security Breach Incident Report Form.
• The equipment must be returned if I leave the employ of Parkhaven Trust and that a final salary deduction may be made if equipment is not returned.
• Failure to comply with the above could lead to disciplinary action or incur financial penalties.

Signed: Dated:</td></tr>
</table>

Appendix 2

Parkhaven Trust IT New Starter Form

New starter form needs to be sent to Julie.Wills@parkhaven.org.uk.

New Starter Name: Click or tap here to enter text.
Start Date: Click or tap to enter a date.
Service/Department: Choose an item.
Job Title: Choose an item.
Access to J Drive: appropriate to job role requested: **Yes** ☐ **No** ☐
Requires same level of access to the J Drive as ? - *(please enter staff member name)*: Click or tap here to enter text.
Parkhaven Email Address Needed: **Yes** ☐ **No** ☐
Type of Email Address Needed: **Microsoft 365** ☐ **Hornet** ☐
RotaMaster Access Needed ***(granted by HR Dept)***: **Yes** ☐ **No** ☐
Person Centred Software Access Needed ***(granted by Service Mgr)***: **Yes** ☐ **No** ☐
Extra equipment to be arranged: Laptop ☐ Mobile Phone ☐ Tablet ☐ Desk Top PC ☐ Other (Please specify) Click or tap here to enter text.
Further Requests: Click or tap here to enter text.
Requesting Manager: Choose an item. Date: Click or tap to enter a date.

Appendix 3

Parkhaven Trust IT Change Request Form for:

Staff Leaver / Staff Job Change or Access Level / Password Reset

Once completed, please send this form to: Julie.Wills@parkhaven.org.uk

Staff Member Account Name: Click or tap here to enter text.

Service/Department: Choose an item.

Type of change required: Choose an item.

Staff Leaver Information

End Date: Click or tap to enter a date.

Special request: ☐ Email to be diverted for xx period *(please specify divert account name)* Click here to enter text.

☐ Message to be added to user account *(please specify)*
Click or tap here to enter text.

☐ Date **User Account** disabled by **Admin, Trust HQ** Choose an item.

☐ Date **RotaMaster** disabled by **HR Dept** *(if applicable)* Choose an item.

☐ Date **PCS** disabled by **Service Manager** *(if applicable)* Choose an item.

☐ Date **PainChek** disabled by **Service Manager** *(if applicable)*
Choose an item.

☐ Date **Paxton** (Staff Badge) disabled by **Service Manager** *(if applicable)*
Choose an item.

☐ Equipment ie Laptop, Mobile Phone etc to be collected by **Service Manager (if applicable) and given to Trust HQ Admin** *(please specify)*
Click or tap here to enter text.

Staff Job Title Change

Date of Change: Click here to enter a date.

New Job Title: Choose an item.

Additional IT requirements required *(please enter below)*:

Form completed by: Date: