PARKHAVEN TRUST

Data Protection Policy: G02

1. Introduction

1.1 In the course of their work employees may come into contact with and use confidential personal information about people. This policy will ensure that employees do not breach data protection legislation including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, (DPA). If employees are in any doubt about what they may or may not do, they should seek advice from their line manager. If they are in doubt and cannot get in touch with their line manager or the Human Resources Manager, they must not disclose the information concerned.

1.2 The Trust holds personal data on all employees relating to their employment, such as names and addresses and on service users, their families, health and other private matters, which is necessary for the management of their care needs. Every effort is made by the Trust to ensure that the accuracy and relevance of this information is maintained. Changes notified by the individual, relatives or other health professional will be acted upon. It is the responsibility of the individual employee to inform their line manager of any information changes so that the relevant records can be updated.

2. Data Protection Law

2.1 Data protection legislation exists to protect 'personal information' this is defined as: *any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (eg: Name, identification number).*

2.2 In addition, the legislation identifies sensitive or 'special category' data that is subject to additional safeguards, this includes information relating to an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

2.3 Data Protection legislation covers both manual and computerised data and information and covers all aspects of processing data: collection, holding, access, use, disclosure and destruction. It requires eight data protection principles to be followed in the handling of personal data. These are, Personal Data:

- must be fairly and lawfully processed.
- processed for a limited purpose and not in any manner incompatible with those purposes.

- must be adequate, relevant and not excessive in its nature.
- must be accurate.
- must not be kept for longer than is necessary.
- must be processed in accordance with individual rights.
- must be held securely
- must not be transferred to countries outside the EU, without adequate protection.

3. Data Controller and Management Responsibilities

3.1 Parkhaven Trust is registered as a data controller with the Information Commissioner. This registration covers the processing of service user/relative data and staff data used for personnel/employee administration, including administration of the staff pension scheme.

3.2 The Chief Executive is accountable to the Board of Trustees for ensuring that the Trust complies with all necessary legislation; however, for operational reasons, this accountability is devolved to Senior Management for their respective roles. The Human Resources Manager is accountable for ensuring that the Trust fulfils its obligations in relation to employment practices and that line managers, who hold individual employee and service user's files, do so in accordance with this policy. The Operations Manager is accountable for ensuring that the Trust fulfils its obligations in relation to the data held on service users. This is dealt with separately under the Care Policy: Record Keeping and Access to Files. Individual line managers are responsible for ensuring that any employee or service user files are maintained in a locked secure place, in accordance with the relevant policy and that their staff and service users are aware of their rights under those policies.

3.3 The Trust will keep the following personal data about all employees: names, address, Date of Birth, National Insurance Number, rate of pay, home / mobile telephone number. This information is obtained from the application form and DBS disclosure form. It will only be disclosed to comply with our legal obligations and for payroll and tax purposes, unless there is a signed declaration authorising disclosure to a third party.

3.4 The Trust may also hold sensitive personal data about employees which may be use for monitoring purposes and to ensure compliance with statutory duties, including, race, union membership and health information.

3.5 If the Trust sells all or part of its business it may provide personal data about employees to any prospective purchaser in the course of negotiations. So far as possible such data will be provided in an anonymous form and if this is not possible the prospective purchaser will be required to keep the information confidential. The Trust will transfer employees' personal data on any transfer or sale falling within the terms of the Transfer of Undertakings (Protection of Employment) Regulations 1981.

3.6 The Trust may keep the following personal data about all service users: names, address, Date of Birth, National Insurance Number, home / mobile telephone number, bank details, relatives contact details, and relatives bank details. This information is obtained to comply with our legal obligations under CQC Standards and to sure the integration of care provided by Parkhaven Trust with other parties or agencies.

3.7 Accessing employee or service user records, either paper or electronic files, without due authority will be treated as gross misconduct and is a criminal offence under Data Protection law.

E-mail or fax.

3.8 Particular attention is drawn to the risks of transmitting confidential information by e-mail or fax. The Trust's Information Technology and Data Security Policy, provides guidance on the appropriate use of e-mails and faxes to reduce the risk; this follows the guidance recommended by the Information Commissioner's Office.

3.9 Documents containing sensitive or 'special category' personal information should only be transmitted between locations if a secure network or comparable arrangements are in place or if, in the case of e-mail, encryption is used.

3.10 Copies of e-mail and fax messages received by managers should be held securely.

3.11 The Information Technology and Data Security Policy, highlights the risk of transmitting employee information by e-mail. Employees must not transfer data to countries outside the European Economic Area (EEA).

3.12 The Trust provides a means by which managers can effectively delete e-mails that they receive or send from the system. It is the responsibility of the individual user to maintain their system appropriately.

3.13 The Trust monitors e-mails and telephone calls but strictly in accordance with what is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This is an implied term in the employee's contract of employment.

4. Retention of Records

4.1 The Trust follows the retention periods recommended by the relevant bodies. In some cases, these retention periods have been extended for a specific business case for example the retention of sickness records for the purpose of calculating Company sick pay entitlement.

4.2 A full list of retention documents and times can be found in the appendix to the Trust's Data Retention Policy.

4.3 Any data protection queries should be addressed to the employee's line manager or the Trust's Data Protection Lead.

5. Security of Manual Records

5.1 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.

5.2 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.

5.3 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.

5.4 It is good practice to maintain a 'clean desk' policy and this should be a part of the above practices.

6. Security of Electronic Records

6.1 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.

6.2 Parkhaven Trust has introduced a computerised Human Resource system which contains sensitive information on employees. To prevent the accidental loss, destruction or disclosure of personal or sensitive data held on computer records will be secured as follows.

6.3 Line managers may only have access to data files for employees they either directly manage or their subordinates manage.

6.4 Access to the computer system will be password protected.

6.5 The computer system will operate an automatic log out after 30 minutes.

6.6 Laptop computers are not secure places to store data and should only be used to access the Parkhaven server rather than store information relating to the Trust, or to Trust employees or service users. Staff must not access the Parkhaven server remotely from a personal computer.

6.7 Where staff access the Parkhaven server remotely from a Trust device the log on and password must not be saved automatically to the computer, but entered personally each time it is used.

6.8 USB memory sticks are not permitted on Trust devices.

6.9 In the event that a laptop or mobile device belonging to the Trust or containing information relating to the Trust or Trust employees or service users, is lost or stolen, the loss should be reported to the line manager immediately, detailing the nature of any personal or sensitive information involved.

6.10 Prior to the destruction or disposal of IT equipment all memory cards and hard drives will be removed and destroyed.

7. Monitoring of Email and Internet Usage

7.1 This is covered in the Information Technology and Data Security Policy, which employees are required to read if they access or use either internet or email or both.

8. Disclosure Requests from Third Parties

8.1 The following process will be observed when the Trust is compelled by law to disclose information and/or data held on employees or service users for example; tax office enquiries or care plans.

8.2 With the exception of inspections (announced or unannounced), where disclosure is in order to comply with a legal duty, all requests should be in writing, and clearly state the basis

on which the legal duty is asserted. The assertion must be verified as correct prior to any disclosure being made.

8.3 Where disclosure is requested (e.g. mortgage request), information will not be given out over the telephone and a written request must be obtained. The signed and explicit consent of the individual must be given to the Trust before this information is released.

8.4 From time to time, an employee may be requested to disclose personal and/or sensitive information about another employee or a service user(s). The following should be adhered to in relation to employment practices and information.

8.5 If the person requesting the information is the line manager of the subject of the request and requires the information to do their job, then comply with their request.

8.6 If the person requesting the information requires the information to do their job, then comply with the request. For example, a request from Wages concerning the off-duty.

8.7 If in doubt clarification should be sought from a Senior Manager before disclosing the information.

8.8 If the person has no need for the information or is not covered by the above, politely refuse and refer them to a Senior Manager. If the person was entitled to the information, employees will not be disciplined for refusing. The issue may be discussed with the employee at supervision to clarify their understanding.

8.9 The Trust has a duty to maintain staff and service users records in a manner which ensures they are available for review, if required. For this reason, the Trust will not agree for files to be removed by a third party, except where there is a legal obligation for the Trust to do so. Access to files may be granted to allow a third party to make photocopies as appropriate, they may be required to cover associated costs.

8.10 Access to files by a third party will be on the basis that the confidential declaration form in appendix 2 of this policy is signed by the individual or on behalf of an organisation accessing the files.

8.11 For information on service users, please refer to the Care Planning and Individual Review Policy and Record Keeping and Access to Files Policy.

9. Rights of the Individual

9.1 Under data protection legislation employees and service users have the following rights:

a. The right of access to records held on them;
b. The right to prevent processing likely to cause unwarranted and substantial damage or distress;
c. The right to prevent processing for the purposes of direct marketing;
d. Rights in relation to automated decision making;
e. Rights to compensation;
f. The right to correction, blocking, erasure or destruction;
g. The right to request an assessment;

9.2 These are subject to the information or data being held in a relevant filing system and providing no exemptions apply. The exemptions relevant to Parkhaven Trust include: crime and taxation (e.g. HMRC, Social Security Benefit information); management forecasting and or management planning; negotiations (notwithstanding those matters covered under trade union and TUPE legislation); corporate finance and confidential references given by Parkhaven Trust.

9.3 All new staff can expect to be told what data and information is held on them, the reason for its retention, who it will be processed by and if it is to be disclosed; where there is no other legitimate reason for disclosure, their explicit consent will be sought prior to the disclosure.

9.4 New service users will be told what data and information is held on them for the purposes of supporting their care needs and any legal requirements.

9.5 The Trust recognises that an individual has a right to access to information and data held on them. Individuals may make a request to have access to the information held on them by the Trust; such requests must be made in writing. Refer to the Subject Access Request policy for further guidance.

9.6 The Trust recognises that managers will need to maintain information on their staff and service users (e.g. contact telephone number, contracted hours, rota and supervision records, medical history). However, this information should be kept to a minimum and the above access protocol must be observed. The Human Resources Manager will manage the request to access a personnel file by an individual.

10. Employee Duties

10.1 Parkhaven Trust delegated responsibilities and accountabilities for Data Protection in accordance with the role and responsibilities of its employees. To enable the Trust to fulfil its duties under the legislation, the Trust has the following rights; to expect that employees will comply with their duties in this policy and that employees will observe strict confidentiality of personal and/or sensitive data regarding information on other employees or service user(s), unless their duties require disclosure and the person to whom the information is disclosed is entitled to that information. Refer to the Safeguarding Policy for further guidance.

10.2 The employee is required to ensure that information given about them on the application form and subsequent documentation is correct and up to date. They must inform the Trust of any changes to the personal data (e.g. address, telephone numbers) so that the Trust can comply with its statutory duties.

10.3 Employees must co-operate with the Trust in fulfilling its legal duties under the legislation and undertake such training as the Trust requires, so that the employee can fulfil their duties and are aware of their rights under the legislation.

10.4 Employees must report the loss or theft of computers which have been used to access the Parkhaven server so that passwords can be changed.

11. Additional information

11.1 This policy has been informed by the Information Commissioner's employment code of practice, "*The use of personal data in employer/employee relationships*" in mind. It is also in accordance with the Trust's duties under the Care Standards Act 2008.

11.2 This policy should be read in conjunction with the Care policy on Confidentiality and Disclosure of Information, Information Technology and Data Security and the relevant section on confidentiality in the employee handbook.

For the avoidance of doubt, this policy does not form part of employees' contracts of employment and may be changed by the Trust at its absolute discretion at any time.

K Randall
Finance Manager
January 2019

Parkhaven Trust - Appendix 1

Retention of Personnel information

Document	**Time Span**
Annual appraisal/assessment records	5 years
Annual leave records	2 years
Application forms and interview notes for unsuccessful applicants	One (1) year
Application forms and interview notes for successful applicants	Six (6) years from the end of employment
Disciplinary Hearings and sanctions	All notes and reports will be placed in a sealed envelope in the personnel file. These are then retained for six (6) years after employment ceases
Parental leave	Five (5) years from birth/adoption of the child or eighteen (18) years if the child receives a disability allowance

Personnel files and training records (including disciplinary records and working time records)	Six (6) years after employment ceases
Record of pensioners	Twelve (12) years after benefit ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State.	Twelve (12) years from the date of redundancy
References given/information to enable references to be provided	Five (5) years from reference/end of employment
Trade union agreements	Ten (10) years after they cease to be effective
Works Council minutes	Six (6) years from the date of the meeting

Parkhaven Trust - Appendix 2

CONFIDENTIAL DECLARATION FORM
Third party access to confidential files

Name of File .....

Details of the individual/organisation accessing the file .....

.....

In accordance with Parkhaven Trust policy, access to confidential files will only be granted upon the signature of the following declaration *(delete as appropriate)*

I ..... / acting on behalf of .....

will ensure that any information made available is used for the purpose of

.....
(state the purpose for which the file is to be used. Nature of any investigation; civil, criminal),

will not be shared with any other parties without prior agreement with Parkhaven Trust. All

information obtained from this file will be handled confidentially and in accordance with appropriate legislation including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Signature of individual accessing the file .....

Date of access .....

Office use

Access concluded and file returned .....

Name of Parkhaven Staff .....

Signature of Staff .....

Date .....