PARKHAVEN TRUST

Data Management Policy: IG01

Contents

1. Introduction

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 Finance & Information Manager, they must not disclose the information concerned.

Parkhaven Trust holds personal data on all employees relating to their employment and on service users relating to the provision of care. Every effort is made by Parkhaven 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.

This policy consists of three elements relating to the General Data Protection Regulation (GDPR). It outlines the rights that individuals have under the GDPR in relation to the data that we hold about them; their right to access the personal data that Parkhaven Trust holds on them and Parkhaven Trust's obligation to report to the Information Commissioner if data under our control is exposed to risk or 'breached'.

The purpose of this policy is also to ensure that information, correspondence and records which are no longer current are stored and promptly disposed of, when appropriate, in an efficient and responsible manner. This will ensure that the organisation has ease of access to current files and that any historical documents can be readily retrieved if required

Individuals, for the purposes of this policy, includes service users, paid staff (current, prospective and former), volunteers, Trustees and contractors.

2. Data Protection Law

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).

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.

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.
- must be 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

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.

The Chief Executive is accountable to the Board of Trustees for ensuring that Parkhaven Trust complies with all necessary legislation; however, for operational reasons, this accountability is devolved to Senior Management for their respective roles. The Human Resources Business Partner is accountable for ensuring that Parkhaven 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. 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.

Parkhaven 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. Parkhaven 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.

Parkhaven Trust may keep the following personal data about all service users: names, address, Date of Birth, health records, 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.

Closed circuit television (CCTV) is installed at The Beeches for the purposes of staff, service user and premises security, safety and good management. All cameras are located in prominent positions within public and staff view and do not infringe on clinical or treatment areas. Signs are displayed in The Beeches to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment.

If Parkhaven 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. Parkhaven 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.

Accessing any employee or service user data, 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.
Particular attention is drawn to the risks of transmitting confidential information by e-mail. Parkhaven 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.

Documents containing sensitive or 'special category' personal information should not be sent by fax. Copies fax messages received by managers should be held securely.

4. Employee Duties

Parkhaven Trust delegate responsibilities and accountabilities for Data Protection in accordance with the role and responsibilities of its employees. To enable Parkhaven Trust to fulfil its duties under the legislation, Parkhaven 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.

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 Parkhaven Trust of any changes to the personal data (e.g. address, telephone numbers) so that the Parkhaven can comply with its statutory duties.

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

Employees must report the loss or theft of Parkhaven Trust devices to their line manager and the data protection lead.

5. Confidentiality

The purpose of this section is to ensure each member of staff is aware of their responsibility not to misuse any information known about Parkhaven Trust, its service users, or other members of staff.

The nature of work in caring for vulnerable people is such that through contact and discussion with service users, their relatives and other professionals, staff become aware of detailed personal information. It is also necessary for staff to be advised of some quite intimate personal details to ensure that appropriate care and attitudes are maintained.

All service users are entitled to the privacy and dignity which we all expect to enjoy and it is essential that all staff respect this.

To accomplish this, whilst it is appropriate to discuss service user details with other involved staff and professionals, this must only be to ensure understanding and the provision of good care. Information about service users must not be misused in any way, nor divulged to any third party unless that person has a legal right to the information.

It is inappropriate to use information known about a service user to ridicule them or to use it for some personal advantage.

On training courses, as part of the learning process, it is usual practice to discuss experiences with and of service users. This must be done without encroaching upon their privacy and dignity by ensuring that it is not possible for anyone to identify the service user from the information given.

All staff will become aware of information about Parkhaven Trust of varying amount and detail. It is essential that staff recognise that divulging information may work to the detriment of Parkhaven Trust and, in so doing, themselves. This does not mean that staff must not talk about Parkhaven Trust or the service they work in but should ensure any such talk does not breach service user confidentiality, is not detrimental, or may not be used by others to the disadvantage Parkhaven Trust.

Staff are legally responsible for keeping all personal and confidential information under their control safe; this includes protecting it from unauthorised disclosure (eg: providing details to a non-relative, speaking where you can be overheard, leaving case notes exposed, etc).

Confidentiality is a fundamental right of service users, failure to comply with this policy could lead to disciplinary action / summary dismissal and may also lead to legal action being taken against you.

In case of emergency information requests from emergency services and hospitals make a note of the contact details to ensure legitimacy and return the call with the requested information. If unsure contact the on call manager. Information should only be provided if in the individual's best interest.

Discussion with representatives of any of the media is restricted to the Chief Executive. This is to ensure that any information given is as accurate as possible to avoid the possibility of misinterpretation.

6 Record keeping & access to files

A record keeping system provides a means of sharing and logging information that aids staff in reviewing service user's progress.

It also ensures accountability and meets the legal requirements placed upon us by various bodies specifically this:

- Serves as a means of planning services to service-users.
- Is a tool for clear communication.
- Demonstrates and defines the professional practice of staff.
- Assists in the development of staff.
- Assists in the development of the worker.
- Contributes to professional accountability.

- Contributes to openness via access to records.

As an organisation, and as individuals, we are all accountable for what we record, write, say and do in the course of our work. If asked to justify our actions, we rely on records to demonstrate the quality of our practice and decision making.

The records belong to Parkhaven Trust. However, all contents should be accessible to the individual service users with the exception of items that are agreed as confidential.

Contents should be objective, accurate and understandable, being as brief as necessary to record only the important facts and information. All records should be written in clear, simple, jargon free English.

All significant information should be recorded as soon as possible after the event and should be initialled and dated by the staff member making the report

When writing comments about service users, please remember that our core values apply, Choice, Dignity, Respect, and Empowerment.

The following records must be kept in the service user's place of residence:

- a pre-admission assessment based on the service users needs
- a plan of care based around the assessment of need.
- a photograph of the service user (with permission).
- a record of basic information to include:

a. the name, address, date of birth and marital status of the service user.
b. the name, address and telephone number of the service user's next of kin or of any person authorised to act on their behalf.
c. the name, address and telephone number of the service user's general practitioner.
d. the name and telephone number of a social worker/ community nurse whose duty is to supervise the welfare of the service user.
e. the date on which the service user entered the service, left the service or died.
f. a record of all medication kept and administered by the service (MAR).
g. a daily record of all care given, family visits.
h. a record of any incident or accident affecting the service user in the service or of any incident which is detrimental to the health and welfare of the service user. This record should include the nature, date and time of the accident or incident, whether medical treatment was required and the name of the person completing the form.
i. a record of any medical interventions required by the service user.
j. a record of preferred place of care, DNAR.
k. a record of incidence of pressure sores or unaccounted marks on the service user's body. Body map
l. a record of falls and of treatment provided.
m. an inventory of all service users' personal belongings must be kept.
n. any specific wishes the service user has about what to do after their death.
o. an accurate account of any monies held in the home/service belonging to the service user and any financial transactions that may occur.

Images from the CCTV footage may be accessed by Parkhaven Trust management for the purposes of staff, service user and premises security, safety and good management.

access must be via the Information Asset owner and documented in the following manner:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing
- The date and time of replacement of the recordings

7. Retention and destruction of records

Parkhaven 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. A full list of retention documents and times can be found in the appendix.

Records should only be retained as long as it is necessary and appropriate to do so. Documents which are no longer current should be removed from general access and stored securely to minimise data risk and maintain an efficient and effective work place. Documents which are no longer required to be kept will be destroyed in an appropriate and secure manner.

Archiving will take place annually. Both manual and electronic filing systems should be reviewed and documents which are no longer current or in use, i.e. older than one year, should be archived.

If a service user leaves a service or has died, their records (including daily notes, care plans, MAR sheets and medication records) should be boxed and sent securely to Parkhaven Trust HQ for archiving. All boxes or files must be sent with a completed Archive Form, which can be found on the j:drive in Information.

Destruction of records will be recorded by the Administrator and checked and authorised by the relevant member of the Senior Management Team.

Documents identified and approved for destruction will be shredded by a certified external provider to securely destroy these records on site.

Electronic archives will be destroyed by the IT Administrator reformatting or destroying CD's or disk drives.

8. Rights of the Individual

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;

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.

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.

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.

Parkhaven 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 Parkhaven Trust; such requests must be made in writing.

Parkhaven 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 Business Partner will manage the request to access a personnel file by an individual.

The Right to be Informed

To keep service users informed about how we use data, we have made a privacy notice available. You can obtain a copy of this privacy notice from the Data Protection Lead or from our website.

The organisation also has a separate privacy notices for job applicants and employees, these are also available from the Data Protection Lead.

Our privacy notices set out:

a) the types of data we hold and the reason for processing the data;
b) our legal basis for processing it;
c) details of who your data is disclosed to and why, including transfers to other countries and additional security safeguards where relevant;
d) how long we keep your data for;
e) where your data comes from;
f) your rights as a data subject;
g) your absolute right to withdraw consent for processing data where consent is the lawful basis for processing your data;
h) your right to make a complaint to the Information Commissioner if you think your rights have been breached;
i) a statement that we do not use automated decision making;
j) contact details of our Data Protection Lead.

The Right of Access

You have the right to access your personal data which is held by us. You can find out more about how to request access to your data by reading the section below, 'Subject Access Request.'.

The Right to 'Correction'

If you discover that data we hold about you is incorrect or incomplete, you have the right to have the data corrected. If you wish to have your data corrected, you should contact our Data Protection Lead.

Usually, Parkhaven Trust will comply with a request to rectify data within one month unless the request is particularly complex, in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period allowed is two months.

If Parkhaven Trust decide not to take any action based on your request, you will be informed. If you disagree with our decisions, you have the right to complain to the Information Commissioner.

Where Parkhaven Trust has disclosed the data to third parties, they will be informed of the rectification unless doing so will cause a disproportionate effect on us.

The Right of 'Erasure'

In certain circumstances, Parkhaven Trust are required to delete the data we hold on you. Those circumstances are:

a) where it is no longer necessary for us to keep the data;
b) where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;
c) where you object to the processing (see below) and the organisation has no over-riding legitimate interest to continue the processing;
d) where we have unlawfully processed your data;
e) where we are required by law to erase the data.

If you wish to make a request for data deletion, you should contact our Data Protection Lead.

Parkhaven Trust will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure unless doing so will cause a disproportionate effect on us.

The Right of 'Restriction'

You have the right to restrict the processing of your data in certain circumstances. Parkhaven Trust will be required to restrict the processing of your personal data in the following circumstances:

a) where you tell us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have ensured that the data is accurate;

b) where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether it is within our legitimate interests to continue processing;
c) when the data has been processed unlawfully;
d) where we no longer need to process the data, but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should contact our Data Protection Lead.

Where data processing is restricted, we will continue to hold the data, but will not process it unless you consent to the processing, the processing is legitimate under another lawful basis or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible, unless to do so will cause a disproportionate effect on us.

You will be informed before any restriction is lifted.

The Right to Data 'Portability'

You have the right to obtain the data that we process on you in a machine-readable format and to transfer it to another party. Where our technology permits, we will transfer the data directly to the other party on your request.

Data which may be transferred is data which:

a) you have provided to us; and
b) is processed because you have provided your consent or because it is needed to perform the employment contract between us; and
c) is processed by automated means.

If you wish to exercise this right, please speak to our Data Protection Lead.

We will respond to a portability request without undue delay, and within one month at the latest, unless the request is complex or we receive several requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period allowed is two months.

We will not charge you for access to your data for this purpose.

You will be informed if we decide not to action your request; for example, if the data does not meet the above criteria. If you disagree with our decisions, you have the right to complain to the Information Commissioner.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

The Right to 'Object'

You have a right to require us to stop processing your data; this is known as data objection.

You may object to processing where it is carried out:

a) in relation to the organisation's legitimate interests;
b) for the performance of a task in the public interest;
c) in the exercise of official authority; or
d) for profiling purposes. For example, in identification of spending patterns or website interest.

If you wish to object, you should do so by contacting our Data Protection Lead.

We may continue to process the data you have objected to in some circumstances; for example, when:

a) we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
b) the processing is required in relation to legal claims made by, or against, us.

If the response to your request is that we will take no action, you will be informed of the reasons.

The Right Not to have Automated Decisions made about You

You have the right not to have decisions made about you solely through automated decision-making, ie: without human involvement. However, the organisation does not make any decisions based on such processes.

9. Making a subject access Request

Subject access requests must be made in writing. If you wish to make a request, please use the Subject Access Request form where possible, (see appendix 2).

You must provide evidence of your identity. If this is not provided, we will contact you to ask that this evidence is provided before we comply with the request.

Third party requests in relation to your data must be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we will contact the third party to ask that this is provided before we comply with the request.

Timescales
Once any required clarification / ID has been received, we will comply with your request without delay and at the latest within one month. Where requests are complex or numerous, we may contact you to advise that an extension of time is required; the maximum extension allowed is two months.

Fee
We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. This fee must be paid for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances. We may also charge a reasonable fee if you request additional copies of the same information. Requests for access to images must be accompanied by a £10 fee (which is non-refundable if the request is declined).

Information You Will Receive
When you make a subject access request, you will be informed of:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipients your personal data has been disclosed to;
- the retention period for storing the personal data or, where this is not possible, our criteria for determining how long we will store it;
- your right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly;
- the existence of automated decision-making (including profiling) if relevant; and
- the safeguards we provide if we transfer personal data to a third country or international organisation.

Circumstances in which Your Request may be Refused

We may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will also be informed of your right to complain to the Information Commissioner.

We may also refuse to deal with your request, or part of it, if we are not required to disclose your information; for example, where it is subject to legal privilege or relates to management planning. Where this is the case, we will inform you that your request cannot be complied with and provide an explanation.

10. Disclosure Requests from Third Parties

The following process will be observed when Parkhaven 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.

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.

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 Parkhaven Trust before this information is released.

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.

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.

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.

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

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.

Parkhaven 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, Parkhaven Trust will not agree for files to be removed by a third party, except where there is a legal obligation for Parkhaven 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.

Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The Press/Media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account

People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The reason for removal
- Any crime incident number to which the images may be relevant
- The place to which the recordings will be taken
- The signature of the collecting police officer, or other relevant official where appropriate
- The date and time of replacement into secure storage of the recordings

Access to files by a third party will be on the basis that the confidential declaration is signed by the individual or on behalf of an organisation accessing the files.

11. Data Breach

Parkhaven Trust make every effort to comply with the General Data Protection Regulation (GDPR), this includes processing data lawfully and ensuring it is kept securely. If data under our control is exposed to risk or ‘breached’, dependent on the

circumstances, we may be obliged to report this to the Information Commissioner and/or the individuals concerned.

Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a data controller / processor;
- sending personal data to an incorrect recipient;
- devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- lack of availability of personal data.
- Using another user's login ID
- Unauthorised disclosure of information
- Leaving confidential / sensitive files out
- Accessing a persons' record inappropriately (e.g. viewing your own or family members, neighbours, friend, etc)
- Writing passwords down

Breach Prevention / Detection

We have implemented measures to assist us in preventing and/or detecting a personal data breach, including:

- Regular system security reviews and penetration testing
- Tight access controls
- Policies and processes to support data security, data handling, retention, etc
- Employee training
- Regular review of the data held under our control

Where a potential weakness is identified, measures are taken to reduce the associated risk until it is within acceptable levels.

Data Incident Reporting

It is essential that all serious untoward incidents that occur are reported appropriately and handled effectively. Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious. The above definition applies irrespective of the media involved and includes both the loss of electronic media and paper records.

All staff must verbally and/or electronically report any actual data incidents or 'near misses' to their Line Manager. The line manager must then ensure a completed Data Incident Reporting Form *(Appendix 3)* is submitted to the Data Protection Lead as soon as possible

All staff, volunteers, associates and contractors involved must fully comply with the ensuing investigation and with any remedial action taken or recommended to prevent re-occurrence.

Investigation into a Suspected or Potential Breach

If we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by our Data Protection who will decide whether notification to the Information Commissioner is required and whether the breach requires individual(s) to be notified.

All investigated data incidents are reviewed and discussed by SMT and reported to the Board of Trustees. The lessons learned are communicated directly to the staff involved and also to the wider workforce where this is deemed necessary or helpful. It is also good management practice to learn reactively from adverse events in terms of staff relations and minimising losses. Incidents can cause pain, suffering and stress to the person(s) affected, their families, friends and work colleagues. There is a moral obligation to uncover the causes of these incidents and to learn from them.

If (serious) incidents are not investigated and appropriate action taken, the organisation could be more vulnerable in terms of civil litigation and even criminal action. Incidents may incur financial penalties, both individually and in aggregate. These penalties can include the indirect costs resulting from incident recording, reporting and investigating, staff replacement, re-training, work interruption, etc.

Serious information security breaches would open the organisation up to possible legal claims from third parties, but also to fines levied by the Information Commissioner's Office. This could harm the organisation's reputation as a strategic partner and a commissioned service provider

When the Information Commissioner will be Notified

In accordance with the GDPR, we will notify the Information Commissioners Office (ICO) of a breach which is likely to pose a risk to people's rights and freedoms; this will be considered on a case-by-case basis. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified to the ICO:

- a description of the nature of the personal data breach including, where possible:the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned
- the name and contact details of our Data Protection Lead where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When the Individual will be Notified

In accordance with the GDPR, we will notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms; this will be considered on a case-by-case basis. A high risk may include where there is an immediate threat of identity theft or where special categories of data are inappropriately disclosed.

This notification will be made without undue delay.

The following information will be provided when a breach is notified to affected individuals:

- a description of the nature of the breach
- the name and contact details of our Data Protection Lead where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects
- any relevant advice that may reduce / prevent adverse impact for the individual

Record of Breaches

The organisation records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, the effects and the remedial action taken.

The Information Governance Lead will monitor the data incident reports, bringing to the attention of the SMT any worrying trends or issues of concern.

12. National Data Opt-Out

Parkhaven Trust reviews all of our data processing on an annual basis to assess if the national data opt-out applies. This is recorded in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies.

If any data processing falls within scope of the National Data Opt-Out we use MESH to check if any of our service users have opted out of their data being used for this purpose.

13. Additional information

This policy should be read in conjunction with the IT and Data Security Policy 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.

Finance & Information Manager
November 2024

Appendix 1: Length of Retention of Records

Finance

Document	Time Span
Payroll records and correspondence with HMRC (including monthly payroll file, pay slips, P60 records)	Not less than six (6) years and a day after the end of the financial year to which they relate
Sales and purchase invoices	Six (6) years after the end of the financial year to which they relate
Bank receipts payments and reconciliations, petty cash records, quarterly management accounts, year end audit file	Six (6) years after the end of the financial year to which they relate
Deceased / former service user financial information	Six (6) years after the end of the financial year to which they relate
Pensioners' records	Twelve (12) years from the ending of any benefit payable under the policy
Money purchase details	Six (6) years after transfer or value taken

Pension

Document	Time Span
Actuarial valuation reports	Permanently
Pension scheme investment policies	Twenty (20) years from the ending of any benefit payable under the policy
Pension Trust deeds and rules	Permanently
Pension Trustees' minute books	Permanently

Human Resources

Document	Time Span
Annual appraisal/assessment records	Five (5) years
Annual leave records	Two (2) years
Application forms and interview notes for unsuccessful applicants	Six (3) months
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 18 years if the child receives a disability allowance

Personnel files and training records (including disciplinary records, working time records and references)	Six (6) years after employment ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	Twelve (12) years from the date of redundancy
Service Contracts for Directors	Three (3) years
SSP certificates and self certificates, SMP and SBP certificates and other evidence	Six (6) years after the end of the financial year to which they relate
Time cards	Two (2) years after the annual leave year to which they refer
Trade union agreements	Ten (10) years after they cease to be effective
Works Council minutes	Permanently

Care

Document	**Time Span**
CQC reports and correspondence	Five (5) years
Report books (including visitor books)	Three (3) years after the last entry
Service users' records (including care plans, daily records, medication reports)	Six (6) years after the date the service user left the service or deceased
CCTV recordings (not required for purposes of staff, service user and premises investigations)	30 days

Legal

Document	**Time Span**
Minutes of meetings with Trade Unions	Permanently
Accident books, accident reports/records	Forty (40) years after the date of the last entry
Medical records as specified by the COSHH regulations 1994	Two (2) years
Record of tests and examinations of control systems and protective equipment under the COSHH regulations 1994	Five (5) years from the date on which the tests were carried out
Employers' Liability Insurance Certificates	Forty (40) years
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently

Estates / Maintenance

Document	**Time Span**
Valuation reports	Six (6) years

Correspondence relating to sold property	Six (6) years
Plans and drawings	Permanently
Planning applications	Forty (40) years
Asbestos surveys	Forty (40) years
Building regulations	Forty (40) years
Safety tests and standards relating to care standards	Forty (40) years
Electrical periodic inspections	Seven (7) years
Inspection reports	Seven (7) years
Services of equipment, including fire extinguishers, lifts and lifting equipment (i.e hoists)	Seven (7) years
Insurance inspections	Seven (7) years
Legionella testing and water testing	Forty (40) years

Trust Board

Document	**Time Span**
Trustee/Board records and correspondence	Permanently
Records of senior executive	Permanently for historical purposes
Trustees	Permanently

Miscellaneous

Document	**Time Span**
Comments and complaints	Three (3) years from date of last entry
Incident forms	Three (3) years from date of last entry
Certificate of motor insurance	Forty (40) years
MOT and service documents	Forty (40) years

Appendix 2: Subject Access Request Form

Title (please tick one):	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Title (please state):
Forename(s):	
Family Name:	
Previous Family Name:	
Other name(s) known by:	
Date of Birth (dd/mm/yyyy):	……../……./……. Male ☐ or Female ☐
Current Address:	
Postcode	
Daytime Telephone No:	
Email Address:	
Previous Address:	
Postcode:	

Section 3 – Proof of the applicant's identity

In order to prove the applicant's identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card

List A (photocopy of one from below)		**List B (plus one <u>original</u> from below) ***	
Passport/Travel Document	☐	Utility bill showing current home address	☐
Photo driving licence	☐	Bank statement or Building Society Book	☐
Foreign National Identity Card	☐		☐

Section 4 – Details of Information Required

Please use this space to give us any details about the information you are requesting, for example by stating specific documents you require (use extra sheets if necessary):

Section 5 – Declaration

The information which I have supplied in this application is correct, and I am the person to whom it relates or a representative acting on his/her behalf. I understand that Parkhaven Trust may need to obtain further information from me/my representative in order to comply with this request.

Signature of Applicant:	Date:

Section 6 – Representative Details

Name of Representative:	
Company Name:	
Address & Postcode:	
Daytime Telephone No:	
Email Address:	

Section 7 – Proof of the Representative's identity

Please provide copies of two pieces of identification, one from list A and one from list B below and indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card

List A (photocopy of one from below)		**List B (plus one <u>original</u> from below)**	
Passport/Travel Document	☐	Utility bill showing current home address	☐
Photo driving licence	☐	Bank statement or Building Society Book	☐
Foreign National Identity Card	☐		☐

	☐		☐
	☐		☐

Section 8 – Authority to release information to a Representative

A representative needs to obtain authority from the applicant before personal data can be released. The representative should obtain the applicant's signature below, or provide a separate note of authority.

This must be an original signature, not a photocopy (tip: using blue ink often helps verification).

If seeking access to information in relation to an applicant who does not have mental capacity to manage their own affairs then evidence of power of attorney or court of protection must be provided.

I hereby give my authority for the representative named in Section 3 of this form to make a Data Subject Right Request on my behalf under Data Protection Legislation.	
Signature of Applicant:	Date:
Signature of Representative:	Date:

Section 9 – Timescale

If you have specific reasons for requiring data by a specific date please give details below:

(a) Date required:
(b) Reason (please state and supply supporting evidence):

Appendix 3: Data Incident Reporting

Section 1 – 4 to be completed by the Line manager and sent to the Data Protection Lead.
Please note that any emails or other documents prepared in connection with this incident must be headed LEGALLY PRIVILEGED AND CONFIDENTIAL. Circulation of such documents must be restricted to those directly involved in investigating the incident. Please do not reference data subjects by name in this report.

Report completed by *[name, job title]*	
Strategic Work Area/Project	
Date of report	

1 Description of data lost, stolen, released or corrupted *[include examples of type of data and volumes of records affected]*

2 Circumstances of the loss, theft, release or corruption *[include timing of events; location; IT hardware and applications involved; details of actions taken to date eg: anyone who has been contacted in relation to the incident]* ***DO <u>NOT</u> CONTACT INDIVIDUALS WHOSE PERSONAL DATA HAS BEEN COMPROMISED WITHOUT DATA PROTECTION LEAD AUTHORISATION***

3 Contact details of any other regulatory body or collaborative partner who may need to be informed *[eg: funder, statutory partners, etc]*

4 Assessment of any related policies, procedures or guidance which have been breached or wider issues *[list any local guidelines or procedures which have not been followed]*

5 Remedial action taken or recommended to prevent a further occurrence (eg: have all relevant staff / contractors / volunteers completed the mandatory IG training?) *[include name of action owner and target dates for completion where appropriate]*	
Remedial action taken:	Date actioned and action owner
Prevention options to be considered:	Target date and action owner

6 Review of incident handling and actions required *[what could be improved eg: communication, speed of response]*	
Improvements to be considered:	Target date and action owner

Senior Information Risk Officer use only	
Incident investigation - actions required:	Target date and action owner
Investigation complete	
SIRO Signature:	Date:

Is there a ***risk*** to the rights and freedoms of individual/s?	YES	NO
Report submitted to the ICO	Date:	
Is there a ***high risk*** to the rights and freedoms of individual/s?	YES	NO
Affected individuals advised	Date:	