Data Protection (GDPR) Policy

Document Owner	Sandra Osbourne
Date Policy Signed Off	February 2024
Owner Signature	Sandra Osbourne

The purpose of this policy is to guide staff in the principles and requirements of Data Protection Legislation and associated General Data Protection Regulations.

We recognise our responsibilities to ensure the safe and appropriate handling of personally identifiable information and operate a Data Breach Policy in the event that our processes do not achieve this. Please refer to the Policy for further information this includes loss of the equipment in which data may be held e.g. laptop/ phone.

We recognise the rights of the individuals about whom we hold personal information and these are addressed in this Policy.

Policy Statement

Narthex Sparkhill is registered with the Information Commissioners Office (ICO) as required by the Data Protection Act 2018 and the General Data Protection Regulations 2016.

The Charity has developed and operates to policies and procedures intended to responsibly and appropriately gather, use, store, share and dispose of personal information associated with our business needs, for which we have a legitimate need or specific consent to process. Our policies, procedures and processes encourage transparency and honesty in all aspects of processing and respect the rights of individuals.

This information includes details about staff, service users and other individuals. The systems and processes we use to handle personal information intend to protect individuals and the Charity from the potential for any misuse of personal information, including loss, inadvertent sharing or use for other than its intended purpose.

Data refers to electronic and hard copy material and information held in all media formats e.g. hard copy document, emails, text messages, voice recording, social media, photographic images, IP addresses, testimonials.

We will ensure that all staff are suitably trained and skilled to recognise their responsibilities within Data Protection and GDPR requirements and enabled to apply these in practice.

Narthex Sparkhill will promote a positive working relationship with the Information Commissioners Officer (ICO) with whom it is registered.

Definitions

Data Protection Legislation From 25 May 2018 the General Data Protection Regulation (GDPR) together with the Data Protection Act 2018 (the Data protection legislation) governs the processing of personal data. The data protection legislation requires that personal data including special categories of personal data, which are regarded as more sensitive, must be processed by data controllers in accordance with the data protection principles set out in the GDPR.

Data Controller and Data Processor Narthex Sparkhill are both a "Data Controller" and a "Data Processor" of personal data.

- A "Data Controller" is any entity (company, organisation or person) that determines the purpose and means of processing personal data e.g. makes its own decisions about how it is going to collect and use the personal data. A Data Controller is responsible for compliance with data protection laws. Examples of personal data we are the controller of are staff details or information we hold about Service Users.
- A "Data Processor" is any entity (company, organisation or person) which accesses or processes personal data on behalf of the data controller.

Information Commissioner's Office (ICO) is the UK's data protection regulator (Lead Supervisory Authority).

Data Breach: when data is lost, stolen, damaged or mistakenly destroyed.
A data breach is defined as any incident that has affected the confidentiality, integrity, or availability of personal data. Any breach that is likely to have an adverse effect on an individual's rights or freedoms must be reported. If you become aware of a data breach, you must contact the HR & Compliance Manager immediately, who will provide advice on further action, and whether the ICO needs to be reported.

Where a report to the ICO must be made, it should be done without undue delay or within 72 hours of the breach being identified. The report must contain the following information:

- Our details.
- Details of the data breach.
- What personal data has been placed at risk.
- What actions have been taken to contain the breach and recover the data.
- What training and guidance has been provided.
- Any previous contact with the ICO.
- Any miscellaneous support information.

We will notify you of any breach that affects your personal data without undue delay. You will be notified to afford you the opportunity to take the necessary steps in order to protect yourself from the effects of the breach. In any such event, we will provide you with the following information:

- The circumstances surrounding the breach.
- The details of who will be managing the breach.
- Any actions we have taken to contain and manage the breach.
- Any other pertinent information that can support you.

Key Risks

We recognise two key areas of risk within the management of personal information:

- Information about individuals being used, or inadvertently shared with unauthorised persons, either from poor security or inappropriate actions, for example:
  - Sharing passwords
  - Releasing attachments to emails without password protection
  - Not checking correct email address
  - Disregarding clear desk policy
  - Retained beyond dates stipulated in the Retention Schedule

- Individuals being harmed through their personal information being inaccurate or insufficient, for example:

  - Service user documentation not having the correct name or contact details and being sent to the wrong person, causing the service user distress
  - Potential impact to service users who are being supported with debt issues if data is not accurate and debt processes are not adhered to within specified time frames.
  - Letters to a member of staff or service user confirming a meeting being sent to a previous address and intercepted by an ex-partner who can now locate them

We will ensure, as far as is reasonably possible, to ensure that our systems, policies, procedures, training and monitoring activities minimise the potential for these risks to be realised.

Penalties for failure to meet Data Protection/ GDPR requirements are specifically defined as:

- Up to 20million euros or 4% of global turnover for Tier 1 (strategic) failures
- Up to 10 million euros or 2% of global turnover for Tier 2 (Operational) failures

Data Protection Officer

Narthex Sparkhill handle sensitive personal information, and as such have appointed a Data Protection Officer.

The Data Protection Officer is responsible to:

- Update the Board of Directors regarding Data Protection/ GDPR responsibilities and requirements
- Review the Data Protection processes, policies, procedures and practices in place
- Advise and support the business with Data Protection/ GDPR issues and queries
- Ensure that Data Protection/ GDPR training takes place, and maintain a record of staff trained
- Handle Subject Access Requests
- Maintain a register of, and support the investigation of, Data Breaches
- Notify Breaches to, and liaise with, the Information Commissioners Office
- Approve unusual or controversial disclosure of personal information
- Review Data Protection/ GDPR element of contracts with Data Processors
- Support with Data Privacy Impact Assessments and Privacy by Design in change projects, innovations and new processes

Personal Information and Confidentiality

The Charity operates a Confidentiality Policy that includes confidential handling of all business information. This section relates particularly to confidentiality within the requirements of Data Protection and GDPR.

In order to conduct its business, The Charity is required to:

- Obtain and process personal data fairly and lawfully
- Hold data only for specified purposes
- Use or disclose data only in a way which is compatible with those purposes
- Ensure that the data held is adequate, relevant and not excessive
- Maintain data accurately
- Keep data only as long as necessary
- Maintain appropriate security measures to any data which is held

All personal information is accessed only on a 'need to know' basis – ability to access does not imply that the information is then used in all cases:

- Staff will have access to information which is relevant and necessary for the safe and effective delivery of service to service users
- Managers and line managers will have access to staff records necessary for the safe and effective management of staff
- Recruitment staff will have access to information generated through staff recruitment activity
- Payroll staff will have access to information required to process pay accurately
- Finance staff will have access to information required to process Invoices accurately
- Marketing staff will have access to customer details generated through marketing activity
- IT staff will have access to all systems held personal information to enable systems support and development
- Quality Auditors will have access to information required in Internal Audits or supporting teams with quality compliance.
- HR staff will have access to information required to manage or support employee relations, business processes and management reporting.
- Recruitment staff and Managers will have access to DBS information as required by Safer Recruitment Standards
  in order to make decisions about recruiting persons with listed cautions or convictions.
- Administration staff will have access to information that supports their line manager in, for example, investigations, report writing, reward and recognition.
- Senior team members will have access to information required to monitor and/or manage significant service issues.

Personal Information will only be accessed where there is a legitimate business need and where the person to whom the data relates understands where and how their information will be accessed, either by acceptance of the Privacy Notice or by giving specific consent.

The Company will share personal information with the relevant authorities where this is in the public interest, regardless of consent, and where there are actual or potential concerns about the safety of any individual or group of people e.g. Safeguarding, Adult Support and Protection, Mental Welfare, Modern Slavery and illegal activity.

In any such instance, the Manager must initially refer to the relevant Policy and follow the guidance therein. Where the situation is not explicitly covered within a Policy, and the Manager is unsure what to do, they should consult with the Data Protection Officer or, in their absence, a senior Operational Manager.

In an emergency situation where any person has been harmed, is at risk of harm, or at risk of causing harm to others, we will give the relevant authorities access to any personal information they require to manage the situation. The Manager does not need to consult in those circumstances but should act in the persons, or public, best interest and update the Data Protection Officer and Senior Operational Manager at the very earliest opportunity.

Transparency - informing people whose information we hold

Narthex Sparkhill recognises its responsibility to inform people about who will have access to their information and for what purpose.

- Service Users will be informed in writing on registering for support with our services. Where the work is in person, a signature will be sought to confirm understanding. For telephone appointments and communications service users will informed and a note will be recorded to that effect. .
- Staff will have this information in their Contract of Employment and Handbook, which they sign. Any updates will be communicated in writing.
- Service Users family members, Next of Kin, Power of Attorneys and legal representatives will have this communicated to them in writing.
- Consent to use personal information for direct marketing or promotional purposes
- Where consent is sought, it will be clear to the individual what they are consenting to, and they shall actively 'opt-in'
- Where consent is given, this only relates to the stated intended use of the information. If there is any desire to use the information for another purpose, further consent must be sought
- Consent may be withdrawn at any time by the individual

We will, on occasion, remind people about using and protecting their information through, formal and informal mechanisms including at service reviews, at supervision meetings, in newsletters, at training and in staff meetings.

Promoting data protection in practice

Narthex Sparkhill have a range of mechanisms to promote best working practices amongst its staff team:

- We operate a Confidentiality Policy that details the manner in which we expect staff to work to maintain confidentiality and integrity
- We train care staff at Induction level and annually thereafter in the principles of confidential working, Data Protection and GDPR
- We require all staff to complete Data Protection and GDPR e-learning which includes confidentiality. The Internal Staff Training Register will be updated and maintained.
- We require all staff to adhere to and promote confidential practice and professional conduct.

Our training encourages staff to think about the information they are using and how to protect this and are advised to escalate any queries or concerns about data handling to their line manager.

Staff who receive a request for information that exceeds what their job role usually requires are aware that this must be escalated to their Manager who will determine, consulting with the Data Protection Officer if necessary, whether the information can be disclosed e.g. requests for information from claims lawyers, Information requests from the regulator.

Authorisation for disclosures not directly related to the reason we have the information

We understand that within the legislation, we are only entitled to have personal information that meets the purpose for which we need it, and we can only use the information we have for that purpose.

If we are asked to disclose information we have for any other purpose, this is likely to fall into one of two categories:

- Information request to support e.g. job application, mortgage application, financial reference, placement reference or similar. We must obtain **written** consent from the person whose information is being requested prior to sharing the data. A copy of the consent must be retained in the relevant HR/ Service User file.
- Information request to inform an official investigation: this must be authorised by a Senior Manager as it may not be appropriate for the person to know that their information is being disclosed, depending on the circumstances e.g. criminal investigation. A written rationale for disclosure without consent must be written and retained on file.

Securing personal information

Security should not be confused with confidentiality. This section relates particularly to security within the requirements of Data Protection and GDPR.

We hold personal information in hard copy and electronic formats, (soft copy) and at times have information for the same person in both formats for specific reasons. These are detailed within the Control of Records Policy and Procedures, which identifies the types of data we hold, document classification, the reason we can hold it, in which formats, how we use It and for how long.

Whether in hard or soft copy, personal information needs to be managed securely by ensuring that:

- Paper records are kept in a recognisable file and filed in an orderly manner.
- Files, when not in use, must be stored in a lockable cabinet, and the keys retained in a keysafe or other secure place. Keys should not be left in cabinets all day as this enables unauthorized access to files.
- Files, when in use, must not be left lying open or unattended and accessible to others: close the file and put in a desk drawer if being left unattended for a short space of time. Return the file to the filing cabinet once no longer required and lock it away.
- When an employee leaves, or a service is no longer required, the file becomes ‘finished’. It must be removed from the cabinet and placed into an archiving box: closed files must be held on site for a minimum of 6 months, then archived. Please refer to the Retention Policy.
- Finished files can be held either in the drawer or in an archiving box that is held securely until it can be sent for archiving: space at the premises will determine which is most practical.
- Electronic information is protected by passwords.
- Passwords are unique to each user and must be updated at prescribed intervals, and in a permitted format.
- Passwords must not be shared
- Different job roles have different access levels and permissions, assigned at the point of employment. Any change to this must be requested by the Line Manager, with reasons for the change request, and signed off by a Senior Manager.

- All copies of documents received through fax or from printers must be disposed of in the confidential waste if not collected within 5 minutes. A person is delegated with the responsibility in each location.
- Incoming post must only be passed to the addressee or other authorised person. It may only be opened by the addressee if marked personal.
- Outgoing post must be checked before issued to ensure all documents are for the attended recipient. Confidential documentation should be sealed in a separate envelope and placed within the envelope that has the recipient address details.
- Remote/ flexible workers must ensure that they handle personal information as securely off site as required on site.
- Internal emails operate within a secure system and any information sent externally must be password protected or otherwise encrypted or made anonymous.
- Archived records – hard copy documents that must be retained as per the Retention Schedule. The Archiving Process must be followed to ensure documents are properly filed for ease of retrieval, if required, and destruction once the due date is reached.
- Where archived records are held electronically in our own systems, these are suitably encrypted or anonymized according to the Retention Schedule.

Exceptions

- **Transferring data outside of the UK** – the Charity does not transfer data out of the UK

Retention and disposal of Records

Records must be kept for the required length of time as per the Control of Records Policy and Procedures. All records covered by the Data Protection Act must be shredded prior to disposal at the end of their retention period. The company has a contract with Shred-it, a nationally recognised secure waste disposal company who provide us with certificates of assurance.

References

The Data Protection Act 2018
General Data Protection Regulations (GDPR) 2016