| Policy No: 03-1514 | Authorised: Zainab Yasin | Date: 15th March 2018 |
|---|---|---|

# POLICY ON THE *GENERAL DATA PROTECTION REGULATIONS (GDPR)*

*This Policy defines the arrangements in place within the Organisation that assures compliance to the requirements of the* General Data Protection Regulations *("GDPR"), as relevant to the Organisation's business interests:*

A: INTRODUCTION:

1. The *General Data Protection Regulations (*henceforth abbreviated to *"GDPR")* addresses certain requirements for all Organisations that collect and process personal data as part of their on-going business operations. Personal data is defined as any information relating to an "identifiable living individual", and will therefore apply to the Organisation's service users, employees and suppliers.

2. The *GDPR* applies to any data recorded in a filing system that allows personal data to be easily accessed. In this respect *GDPR* will apply to any of the following types of file where data may be stored:

   2.1 "Hard copy" (paper) files relating to employees (e.g. employment records, safeguarding records, risk assessments, care planning, and other documents requiring original signatures).

   2.2 "Hard copy" (paper) files relating to service users that are routinely kept at the service user's home (e.g. records of assessments of need, medicine records, risk assessments, care planning, and other documents requiring original signatures).

   2.3 Electronic (computer) files relating to staffing issues, (shift allocation, staff skills, training), complaints etc, and service user issues (care planning, environmental risk assessments, accidents etc).

   2.4 Digital image files relating to the following:

   - photographs of staff - for ID badges / verification of identity as part of employment vetting
   - photographs of service users - Care Plan / medicine assistance verification of identity / CCTV images
   - biometric scans - fingerprint scans for door entry systems

B: PRINCIPLES OF DATA PROTECTION:

1. The way in which the Organisation handles and manages service user information will conform to the following 6 principles of Information Management:

   1. Justify the purpose(s) of using confidential information;
   2. Only use it when absolutely necessary;
   3. Use the minimum that is required;
   4. Access to be on a strict need-to-know basis;
   5. Everyone should understand his or her responsibilities;
   6. Understand and comply with the law.

2. The Organisation is committed to the enforcement of the following Code of Good Practice in relation to the data it retains on service users and employees. In summary, data will:

   - be fairly and lawfully processed;
   - be used for a limited and well-explained purpose;
   - be relevant to the Organisation's needs;
   - not be unnecessarily excessive in detail;
   - be accurately maintained;
   - not be kept any longer than is necessary, or as required by law;

- only be used in accordance with the individual subject's rights;
- be securely stored;
- only be made available to authorised persons.

3. In this respect the following additional policies within the Organisation's documentation system are relevant:

- *Policy No 1500: Control of Records & Service Users' Access to Personal Files*
- *Policy No 1501: Records Maintained at the Service User's Home*
- *Policy No 1505: Confidentiality Policy*
- *Policy No 1506: Information Security Policy*
- *Policy No 1508: Electronic Communications Policy* - Code of Practice
- *Policy No 1512: Information Governance Policy*
- *Policy No 3103 Service User* - Privacy
- *Policy No 4300: Business Continuity Planning Policy*

C: POLICY DETAILS:

1. The Organisation will require written consent from the subject individual in order for personal data to be collected, processed and stored. In this respect it will be taken that consent is implied through the following:

1.1 *Service users* - by the service user accepting the Contract for Care, which is signed by the service user or authorised representative. In order for the Organisation to develop an appropriate Plan of Care personal details must be divulged and kept on record. In this respect *Policy Nos 1500 & 1505* (above) are relevant.

1.2 *Employees* - by completing the Job Application Form at onset of the recruitment process, and where the employee has not registered an objection to their data being used.

2. All individuals, service users and employees, have the right of access to manual, electronic and digital records that are relevant to their personal data. For service users, this is supported by *Policy No 1500.*

3. Where it is deemed necessary to divulge personal data to a third party this will only be done with the express permission of the individual subject, ref. *Confidentiality Policy, No 1505. In this respect both staff and service users / relatives / advocates will also be advised that personal information held by the Organisation may be shared with the Registration / Regulating Authority, as appropriate.*

4. The Organisation is committed to understanding and respecting the rights of the individual with respect to the safe and secure handling, storing and management of that individual's personal data. The GDPR will therefore uphold the following fundamental rights for individuals concerning their personal data:

- the right to be kept informed
- the right of access to data at any reasonable time
- the right to rectification of records
- the right to erase / redact any information
- the right to restrict processing of data (e.g. on a "need-to-know" basis)
- the right to data portability
- the right to object to any part of the data content

5. Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records can be in hard copy (paper) format, or as electronic (word processed and scanned *pdf* files), or as digital files (biometric scans and digital photographs). In each case *Policy No 1500* refers, and particular attention is paid to the following aspects of data sharing and storage:

5.1 Hard Copy (paper) files:

- location of storage;
- identification of those employees authorised to have access to specific data;
- service users / advocates authorised to have access to their personal records;
- responsibilities for secure storage of the data at the Organisation;
- accessibility of records at the service user's home;
- retention times; i.e. how long data records are kept for.

5.2 Electronic (computer) files:

- responsibilities for implementing data security systems for computer files;
- password-protection for access to sensitive data files;
- who is authorised to have knowledge of these passwords;
- how often passwords are changed;
- implications for networked systems;
- how long data records are kept for (retention times);
- back-up, control and management of personal data files;
- any special control requirements needed when on-line back-up services are used.

5.3 Digital files (photographs, CCTV and biometric scans):

- responsibilities for implementing security systems for digital files;
- password-protection for access to sensitive data files;
- who is authorised to have knowledge of these passwords;
- how often passwords are changed;
- how long records are kept for;
- procedures for the control and management of personal data.

6. When personal data is being processed, administrative staff will take all reasonable precautions to prevent access to data by unauthorised persons:

6.1 Record files are locked away when not required, ensuring that computer / biometric files are password-protected and that passwords are regularly changed.

6.2 Where practical, computer VDU screens are tilted towards the user and away from the general office environment.

6.3 VDUs are not left on when not in use – switched off / locked.

6.4 Managing a "clear desk" policy for personal office housekeeping, ensuring that confidential electronic files are encrypted when not in use, and that waste confidential paper is destroyed by cross-cut shredding.

6.5 Ensuring that confidential conversations are not overheard.

6.6 Ensuring that information is transported securely.

7. **Privacy Impact Assessments / Data Protection Impact Assessments:**

Privacy Impact Assessments (PIAs), or Data Protection Impact Assessments (DPIAs), help Organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

7.1 Privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective PIA uses existing project management processes to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

7.2 **Privacy**, ref. *Policy No: 3103*, is about the right of an individual to be left alone. There are 2 types of privacy, each subject to different types of intrusion:

- *Physical privacy* - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance, and the taking of biometric information.

- *Informational privacy* - the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

7.3 **Privacy risk** - the risk of harm arising through an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to, or unexpected by, the person it is about;
- not kept securely.

7.4 Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It can contribute to a loss of personal autonomy or dignity, or exacerbate fears of excessive surveillance.

7.5 The outcome of a PIA should be a minimisation of privacy risk. As such, the Organisation will develop an understanding of how it will approach the broad topics of privacy and privacy risks for its service users and staff. Understanding privacy risk in this context requires an understanding of the relationship between an individual and the Organisation, and factors that can have a bearing on this include the following:

- reasonable expectations of how the activity of individuals will be monitored.
- reasonable expectations of the level of interaction between an individual and an organisation.
- the level of understanding of how and why particular decisions are made about people.

7.6 **The projected benefits of a PIA** - it is the Organisation's objective that undertaking an effective PIA should benefit the people affected by the project and also the organisation carrying out the project. Benefits can include the following:

- It will demonstrate to the *ICO (Information Commissioner's Office)* how personal data processing complies with legal requirements, and that individuals can be reassured that the organisations which use their information have followed best practice.

- A project which has been PIA assessed should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

- A PIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

- Undertaking the assessment will improve how the Organisation uses information which impacts on individual privacy. This should in turn reduce the likelihood of the Organisation failing to meet its legal obligations.

7.7 Conducting and publicising a PIA will help our Organisation to build trust with our service users. The actions taken during and after the PIA process can improve our understanding of our service users. There can be financial benefits to conducting a PIA. Identifying a problem early will generally require a simpler and less costly solution. A PIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used where this is possible, and devising more straightforward processes for staff. Consistent use of PIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of a project.

7.8 **Projects which might require a PIA - t**he core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals. These can include the following:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- Any new surveillance system or the application of new technology to an existing system
- A new database which consolidates information held by separate parts of an organisation.