DATA PROTECTION

POLICY AND PRACTICE GUIDANCE

VERSION	**v1.10**
REVIEWED	**January 2025**
REVIEW DUE	**January 2026**

DATA PROTECTION

POLICY AND PRACTICE GUIDANCE

1. Policy Statement

In order to operate efficiently, A+bility Limited has to collect and use information about people with whom we work. These include, but are not limited to, service users (and families/carers), staff, contractors, commissioners and partner organisations.

A+bility Limited is committed to providing a confidential service to all.

A+bility Limited believes that principles of confidentiality must be integrated across all aspects of services and management and believes its users deserve the right to confidentiality to protect their interests and safeguard A+bility Limited's services.

The Designated Individual for Information Management is Fiona White, Director.

2. Legal Basis

Ability Limited fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR). This applies to all personal information collected and held by the Company – in whatever format and however it is stored.

Staff:
We are required to ask for and store information to enable us to offer staff a contract under Employment law, and to carry out checks required by Safeguarding legislation and good practice.

Service Users:
We are required to ask for and store information that enables us to provide you with a safe and personal service that meets your individual needs. This information is required by contracts we have with the organisation commissioning the service.

3. Purpose

This policy is designed to assure that staff, associates and volunteers are aware of the importance of confidentiality and identify the responsibilities of each person, and to establish procedures to ensure confidentiality is maintained.

A+bility Limited is registered with the Information Commissioners Office (ICO). This is an independent authority which upholds information rights in the public interest, and supports us to comply fully with our Data Protection duties. As we collect and store personal information on individuals (staff and service users), registration with the ICO is a statutory requirement and is renewed annually.

A+bility Limited encourages the use of email, WhatsApp and the internet where it supports the aims and objectives of the company. The Company uses two secure computer systems – Sharepoint and Care Control – to record and store information about Staff and Service Users. This Policy should be read in conjunction with our Email, Internet and Social Media Acceptable Use Notice, this is issued to staff on Induction.

4. Scope

This policy applies to all A+bility Limited staff, associates and volunteers. It refers to all personal information kept on service users, staff and Company financial information. This policy does not prevent the disclosure of information to the police or regulatory authorities if such a disclosure would prevent a prohibited act or inform an investigation.

5. Context

5.1 Confidentiality rests with the company not individual workers, so it is acceptable for all staff, associates and volunteers to have access to those case records necessary to their tasks and to take part in discussions relating to the service users. Administration and clerical workers will also have access to service user details so must be made aware of the Data Protection Policy. Staff files are on a drive that only managers and designated administrative staff can access.

5.2 In order to manage our electronic information management systems robustly and securely, the Company has carefully selected a contractor who understands the care industry. Until 2024, the Company's date was saved on a server and all Company account emails were protected by the same security system. Since February 2024, the company has stored electronic information on two systems. All reports, service user Care Plans and RA's are recorded on Care Control. This is a system designed specifically for the Care Sector and the company ensures the highest level of security. All other Management Data is now stored in the Cloud, via Sharepoint. The contractor also checks the security of Company mobile phones and laptops. The contractor sets up staff accounts on the Cloud, and allows different levels of access only with the permission of a Director or senior manager. The contractor also blocks access on the day a member of staff leaves. A+bility managers and admin staff set up access to service user information on Care Control.

5.3 This policy sets out the Company's procedures to meet their obligations as set out in the following legislation:

The Data Protection Act 2018 (DPA) – This Act makes provision for the regulation of the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information.

The DPA and the UK GDPR should be read "side by side".

The Privacy and Electronic Communication Regulations sit alongside the DPA and UK GDPR. They give individuals specific rights in relation to electronic communications.

The Freedom of Information Act gives people the right to access recorded information by public sector organisations.

5.4 By adhering to the requirements of the ICO registration, the Company ensures compliance.

Under UK GDPR anyone processing personal date must comply with the seven principles which are legally enforceable and require that:

Personal information shall be processed lawfully, fairly and transparently

Personal Information shall be processed specifically, explicitly and legitimately

Personal information held shall be adequate, relevant and not excessive

Personal information held is accurate and kept up to date

Personal information shall be kept for no longer than is necessary

Personal information shall be processed and stored in a manner that ensures appropriate security

The Company shall be accountable and able to demonstrate compliance with the above.

Respecting the rights of the individual

THESE RIGHTS INCLUDE

The right of access to a copy of the information held on them

The right to object to processing personal data that is likely to cause or is causing damage or distress

The right to prevent processing for direct marketing

The right to object to decisions being taken by automated means

The right to have inaccurate data rectified, blocked, erased or destroyed in some circumstances

The right to claim compensation for damages caused by a breach of the Data Protection Act

6. Definition

A+bility Limited understands confidentiality to mean that no information regarding a service user shall be given directly or indirectly to any third party who is external to the staff, managers and directors without that service user's prior expressed consent to disclose such information. The exception is where it is believed someone is suffering or likely to suffer harm. Confidentiality means that information is accessed on a need-to-know basis only.

7. Procedures

7.1 All staff will read and sign to confirm they have understood the policy. This policy will inform induction training on data protection and the need to maintain data integrity and confidentiality.

7.2 All staff receive training at Induction to ensure understanding of their responsibilities under this Policy.

7.3 All personal information on staff and service users, including records made by staff, will be recorded electronically and stored either on Sharepoint or Care Control. Staff are given necessary access to these. Their access is limited on the final day of their employment.

7.4 Only those documents containing personal information needed for business continuity will be kept as paper documents. These will be kept in a locked filing cabinet, and the office locked when no staff are in attendance.

7.5 All documents must be locked away at the end of each working day, including those in 'in trays'.

7.6 All staff and Managers are clearly instructed that they should only access case Records and staff files for business purposes.

7.7 Electronic staff files are stored in a folder on Sharepoint which is only accessible to Managers and Admin staff.

7.8 When disposing of any IT equipment it will be wiped clean by the Company's IT contractor.

7.9 Staff are provided with a secure email address and documents are transferred between staff and head office by email using only company email addresses as this system of transit is secure. The email address and access to records are disabled immediately a member of staff leaves the company.

Staff are advised that email accounts are monitored by managers to ensure compliance.

Company laptops are encrypted.

7.10 Where mobile phones and other devices are used to access work emails,

WhatsApp messages and/or to take photographs of service users, those phones must be password protected using digits not patterns, or biometrics.

The Administration Officer ensures the safe return of mobile phones, laptops ID cards and all other equipment and information, on the last day of employment when a staff member leaves.

Following the introduction of the Care Control (CC) system of recording data our staff have received instruction on how to transmit data. Staff can only access the data they need to about the service users they actually support. Their access to the system is cancelled when they leave A+bility's employment.

7.11 It is good practice to record a service user's activities and achievements by the taking of photographs and videos providing consent has been given for this. Where personal mobile phones are used for this, the images are posted to Care Control, and then deleted from the telephone asap.

7.12 Electronic documents in transit use the person's initials only, unless it is by email between staff who have a work email address, or unless a secure method is used such as Egress. Gloucestershire County Council employees use Microsoft 365 Encryption and documents and emails can be transmitted using this safe service. Documents containing personal data which cannot be transferred using a secure encrypted service are password protected.

It is forbidden to use memory sticks, external hard drives and CD/DVDs to transport or store personal data. Staff can only transfer documents when permission has been gained from a manager, and the means of transfer agreed.

7.13 Only authorised transfer of personal data can be actioned. This will depend on the service user's legal status, which is clearly stated on the case information sheet and the information and consents form which also identifies the parameters for information sharing, and no information can be transferred by staff without permission from a manager.

Emailed documents must be encrypted. The office will provide the receiving agency with a password if encryption is not possible. Where possible the password is provided to the recipient by other means than email.

7.14 Printing of documents containing personal data is done using the networked printers only. These printers are sited in secure offices, next to the computers. The operator printing the document must secure the document immediately.

7.15 Cases will not be discussed outside of the working environment even when not using the service user's name; likewise staff personal details will not be discussed.

7.16 No details on staff or service users will be stored on computer hard drives.

7.17 Service users are informed of the information kept on them on admission, and are also advised of their rights to read what is contained in their files. A brief summary is on the Information and Consents form, and service users will be given the Company privacy notice, a simple to read privacy notice is also available. Information is only retained if it is required to provide a service to the service user.

7.18 Staff are issued with a Privacy Notice which they sign. Information is retained to ensure compliance with Employment Law and Safeguarding requirements. Other information will be retained only if consent is given.

7.19 The Company does not use faxes as this is an unsafe method of transferring information. Neither fax machines nor fax programmes on computers are employed.

7.20 Where information is exchanged by work mobile phones this is done using WhatsApp which is end-to-end encrypted. Staff must not use surnames, addresses or any other personal details that could identify a service user. Only given (first) names or initials should be used. Any letters should be added to CC, NOT posted in WhatsApp, as they might identify a service user's address or other personal information. If for any reason urgent correspondence can only be transferred by WhatsApp then the Service User's personal details, including address, must be blacked out.

7.21 For record retention rules see the Register of Personal Data Held By A+bility Limited which also records retention and disposal details.

7.22 Visitors and contractors to the Office are signed in by Office staff.

Visitors and Contractors are supervised to ensure they do not have access to any information they are not authorised to see.

On completion of their business they sign out and are seen off the premises.

7.23 Breach of these procedures is taken very seriously and might result in disciplinary action

8. Information sharing

The Company may share information when it is in the best interests of the data subject and when failure to share information may carry risks to vulnerable groups and/or individuals. This must be done in a secure and appropriate manner. The Company will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards. When information is shared with other organisations or partners, a specific information sharing agreement should be put in place. Responsibility for its implementation lies with the Information Asset Owner.

8.1 Disclosure of personal information about third parties

The personal data of a third party must not be disclosed, except in accordance with the GDPR. If you believe it is necessary to disclose information about a third party to a person requesting data, you must first seek advice from one of the Directors.

9. Security, Incident Management and Breaches

9.1 Staff, volunteers, associates, service users and customers are able to report information security risks, concerns and incidents to the duty manager, available 24:7 on the office telephone number.

9.2 Information security issues must be reported promptly and if there is a cyber security issue such as a potential cyber-attack then Pearce IT must be contacted immediately.

9.3 The duty manager will take full details of the issue, and make a written record.

9.4 The report will be sent immediately to the Directors who will have an urgent discussion to decide on actions. Actions might include an investigation, in which case one director will take responsibility for investigating and writing a report. Actions include making a report to the I.C.O (Information Commissioner's Office) about the breach within 72 hours.

9.5 Breaches of a service user's confidentiality must be notified to the commissioning agency within 24 hours, and the ICO must be notified within 72 hours.

9.6 Breaches of a staff member's information must be notified to the staff member within 24 hours of the breach being identified, and the ICO must be notified within 72 hours.

9.7 The Manager and Directors will keep a log of the incident, the decision made, actions taken and mitigating measures put in place.

9.8 The Manager and Directors will complete a recorded risk assessment covering:

- How the breach occurred
- What data has been compromised: type, sensitivity and volume
- Who is affected
- How many people it affects
- Whether people are identified in the breached data
- Who has the data

- Whether the incident is contained
- What mitigating action we can take (such as being confident that the person who received the information in error has deleted if from their system).

9.9 If the breach is because of a cyber-attack, the Action Fraud police service must be informed (Police: Action Fraud).

9.10 If it is unclear about who to notify, there is interactive guidance on Where to Report a Cyber Incident at Gov.Uk (Cyber Reporting).

9.11 The report, log, risk assessment and advice and recommendations from other agencies will be considered at Board with a view to identifying areas for improvement and learning and disseminating to all staff. Policies and procedures will be reviewed, amended and disseminated as necessary.

10. Subject Access Requests

If a current member of staff wishes to have sight of their staff file, they can submit their request by email or telephone to their supervisor. Their supervisor will check with the Data Controller (Sally Jackaman) when the file can be made available, and book an appointment to read their paper and electronic files. Staff can then request that their records are updated and amended if necessary.

If a current service user wishes to see their file, a Manager will discuss this request with the case holder where appropriate, to identify documents that should be included or withheld. Documents or information is withheld or redacted to protect the right of others mentioned in the file (such as other family members). If copies of reports written by professionals of other agencies are held, a discussion will take place regarding whether the other agencies require separate subject access requests relating to those documents. Once agreement has been reached, the service user will be given access to their file and a member of staff known to them will be at hand to manage queries, help with reading etc. The service user can request that information is updated and amended.

Information on ex-service users and staff is stored in line with Ofsted and CQC requirements, and financial requirements in the case of payroll information. Ex-service users and ex-staff will be provided with a Subject Access Request form but they can also request access verbally or in writing. This will be processed promptly and in any case within one month, and the information they are entitled to see and have a copy of will then be made available to them.

11. Freedom of Information Requests (FoIR)

If any Placing Authority receives a FoIR then the duty manager will ensure that the request will be dealt with promptly.

All written requests for access to information will be dealt with according to the Freedom of Information Act (FoI) and/or Environmental Information Regulations (EIR).

12. Monitoring and Review

Staff are invited to recommend amendments to any policy at any time. All policies are reviewed by the management team annually. Amendments are disseminated to staff