Confidentiality and Data Protection Policy

1. Aims and Objectives

1.1. This policy outlines how Assessment Services Ltd ensures that personal information is kept secure and confidential, without compromising necessary information sharing.

1.2. It sets out the principles that must be observed by all individuals working with the organisation—including employees, partners, and contractors—who have access to personal data.

1.3. Assessment Services Ltd is committed to protecting all personal information it handles. Information shared in confidence will not be used for other purposes or disclosed to third parties without consent, except under exceptional circumstances (e.g., to prevent harm).

1.4. Personal information will be obtained, used, and disclosed in compliance with the common law duty of confidentiality and the General Data Protection Regulation (GDPR)**.**

1.5. The organisation will adhere to all current and future legal requirements concerning:

- 1.5.1. The confidentiality of personal information in general.
- 1.5.2. Specific categories of personal information (e.g., regarding the Rehabilitation of Offenders Act).

2. Principles

2.1 In line with the **Data Protection Act 2018**, all personal information (manual or electronic) will:

- Be obtained and processed fairly and lawfully.
- Be used only for the purposes for which it was collected.
- Be adequate, relevant, and not excessive.
- Be accurate and updated as necessary.
- Not be kept longer than necessary.
- Be processed in accordance with individuals' rights.
- Be protected from unauthorised access, loss, or damage.
- Not be transferred to countries lacking adequate data protection standards.

3. Definitions

3.1. Confidentiality applies to any information acquired formally, informally, or incidentally. It covers:

- Organisational business
- Employees and potential employees
- Partners
- Customers
- Individuals and external organisations

3.2. Confidential information generally includes:

- 3.2.1. Personal and sensitive data that could lead to discrimination, harassment, or harm if misused.
- 3.2.2. Organisational information that could jeopardise the organisation or partners if disclosed inappropriately.

3.3. Confidentiality breaches occur when sensitive information is accessed or shared without proper authorisation—often due to a lack of procedures or non-compliance with them.

4. Informed Consent

4.1. In exceptional cases, where information may need to be shared with a third party, informed consent should be obtained.

4.2. Consent must be specific: the individual should know what data will be shared, with whom, and for what purpose.

4.3. Confidential information will only be shared when necessary and with explicit, informed consent.

4.4. Consent should be recorded in writing whenever possible, outlining the terms for sharing and storing data.

4.5. Consent must be re-obtained for each new disclosure unless previously agreed.

4.6. Information will not be shared over the telephone unless the caller's identity is verified, using methods such as call-backs or security checks.

4.7. If an individual refuses consent, this will be respected unless legally overridden.

5. Employee Responsibilities

5.1 Permitted Disclosures

Employees may only disclose personal data externally if:

- 5.1.1. The disclosure is a routine requirement, and the individual is aware or could reasonably expect this.
- 5.1.2. Disclosure is required by law.
- 5.1.3. The receiving person has a legitimate 'need to know' to fulfil their duties.
- 5.1.4. The individual has given valid consent.

5.2 Permitted Disclosures

5.2.1 If consent cannot be obtained, disclosure may be made under lawful exceptions, including:

- Court orders or cooperation with law enforcement.
- Agreed inter-agency procedures with a legal foundation (e.g., safeguarding, public protection).
- Overriding public interest, e.g., to prevent serious harm or detect serious crime.

5.3 Sharing Information

5.3.1 When disclosing information:

- Confirm the request is genuine.
- Ensure the recipient agrees to maintain confidentiality.
- Only share what is strictly necessary.
- Record details of the disclosure (what, to whom, when, and why).

5.4 Receiving Information

When receiving confidential data:

- 5.4.1. Mark and handle it as confidential.
- 5.4.2. Only request data essential for the intended purpose.
- 5.4.3. Include a confidentiality statement, e.g.:

"Information will be treated with utmost confidence and will not be shared outside the organisation except where previously stated or agreed. All information will be handled in accordance with Assessment Services Ltd.'s Confidentiality and Data Protection Policy."

5.5 Staff Contracts

All employee job descriptions and partner contracts must include clauses enforcing the duty to protect confidential information.

5.6 Declarations

Staff and partners must sign a confidentiality agreement upon joining the organisation, either within the employment contract or as a separate document.

5.7 Data Accuracy

Employees and partners are responsible for:

- 5.7.1. Ensuring the personal data, they submit is accurate and current.
- 5.7.2. Updating the organisation if their details change (e.g., address updates).

5.8 Sensitive Information Handling

Sensitive data will only be collected when essential to service delivery and based on a clear 'need to know' justification.

6. Change History and Review

Policy Updated: 7th July 2025
Next update due by: July 2026