Confidentiality and Data Protection Policy

1. Aims and Objectives

1.1. This policy is set out to identify how Assessment Services Ltd executes its duty to keep personal information safe and confidential whilst at the same time, not compromising its ability to share information where it is needed.

1.2. The purpose of this **Confidentiality and Data Protection Policy** is to lay down the principles that must be observed by all who work within the organisation including partners and have access to personal information.

1.3. Assessment Services Ltd is committed to maintaining the confidentiality of personal information that it handles. Any information given or received in confidence for one purpose will not be used for another purpose, or passed to a third party, without their consent except in special circumstances e.g. to prevent harm to an individual.

1.4. Assessment Services Ltd will ensure that personal information is obtained, used and disclosed in accordance with the common law duty of confidentiality and the General Data Protection Regulation.

1.5. Assessment Services Ltd will also have full regard for current and future legal requirements which impinge on the confidentiality of:

1.5.1. Personal information in general, and

1.5.2. Specific categories of personal information e.g. rehabilitation of offenders.

2. Principles

In accordance with the Principles of the Data Protection Act 2018, personal information held in both computerised and manually filed records will: -

2.1. Be obtained and processed fairly and lawfully,

2.2. Be used only for the specified purposes for which it was obtained and not in any manner incompatible with those purposes,

2.3. Be adequate, relevant and not excessive for those purposes,

2.4. Be kept accurate and where necessary up to date,

2.5. Not be kept longer than is necessary for those purposes,

2.6. Be processed in accordance with individuals' rights under the Act,

2.7. Be protected from unauthorised access, unlawful processing, accidental loss, destruction or damage,

2.8. Not be transferred to a country which does not ensure adequate protection for the rights of individuals in relation to the processing of personal information.

3. Definitions

3.1. 'Confidentiality' applies to information whether received through formal channels (e.g. in a formal report), informally, or discovered by accident. It applies to organisational business,
employees and potential employees, partner, customers, individuals, or other organisations who come into contact with the organisation.

3.2. Information, which can be classified as 'Confidential' can broadly be grouped into the following areas:

3.2.1. Information of a specific and personal nature about customers, employees or partners. If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others.

3.2.2. Sensitive organisational information. This may be used to damage the organisation and other organisations, as well as individuals, staff or partners. It may be prejudicial to the business of the organisation or used to threaten the security of its property and systems.

a. Breaches in confidentiality happen when sensitive information is given to people who are not authorised to access it. They are most likely to happen when procedures have not been agreed or followed. They can also happen when information is passed between sections, departments or organisations, or when information is being stored insecurely.

4. Informed Consent

4.1. Where it is proposed, in exceptional circumstances, that information about an individual should be shared with another agency or person, the consent of the individual, or the person who provided the information, should normally be sought.

4.2. This should be done in such a way that those persons know exactly what information will be passed on, to whom and for what purpose.

4.3. Information which is confidential and restricted will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

4.4. Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information.

4.5. Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person.

4.6. Confidential information will not be discussed on the telephone unless the identity of the caller is established, this will be checked when necessary, e.g. with call-backs and/or security checks prior to the release of any information.

4.7. Refusal to give consent should be respected wherever possible.

5. Employee Responsibilities

5.1. In normal circumstances, staff may only disclose personal information outside the organisation if one or more of the following applies:

5.1.1. The disclosure is routinely necessary for the purpose for which the information is held and the individuals about whom the data is held have been made aware of, or could reasonably expect, such a disclosure to be made;

5.1.2. The disclosure is a legal requirement under the legislation governing the operation of the service or function concerned;

5.1.3. The receiving staff member 'needs to know' the information in order to carry out their duties;

5.1.4. The person about whom the information is held has given valid consent to the disclosure

5.2. Where it is not possible to obtain valid consent, information may exceptionally be passed on when there is a legal basis for overriding the usual non-disclosure e.g.

5.2.1. The disclosure is required under direction of a Court Order, or in the course of law enforcement, e.g. Trading Standards co-operation with other law enforcement agencies;

5.2.2. The disclosure is provided for agreed inter-agency procedures which have a legal basis for their operation, e.g. Safeguarding Children Board, Sex Offenders Register, Mental Health Supervision Register, Public Protection Unit and other inter-agency procedures for the assessment and management of high risk individuals;

5.2.3. Where this is an overriding public interest in disclosing the information such as evidence of a risk of serious harm to the individual or in order to prevent or detect a serious crime.

5.3. When passing information to others, staff should:

5.3.1. Check that the source of the request is bona fide;

5.3.2. Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;

5.3.3. Only send the information necessary for the purpose of the disclosure;

5.3.4. Record exactly what has been passed on, to whom, when and why.

5.4. When receiving information from others, staff should:

5.4.1. Ensure that any information received in confidence should be marked as such to ensure it is not inadvertently disclosed to third parties;

5.4.2. Ensure that only information necessary for the purpose of the information being shared should be requested.

5.4.3. Ensure that information requests include a confidentiality statement similar to

"Information will be treated with utmost confidence and will not be divulged to anyone outside the organisation except when stated at collection or agreed at a later date." All confidential information shall be treated in line with Assessment Services Ltd Ltd Confidentiality and Data Protection policy.

5.5. All staff employment job descriptions and Partner contracts must contain a statement enforcing the duty to respect the confidentiality of information.

5.6. Staff and partners will be asked to sign declarations of confidentiality on commencing employment with Assessment Services Ltd Ltd either as part of their staff contract or as a separate statement.

5.7. All employees and partners are responsible for:

5.7.1. Checking that any personal data that they provide to Assessment Services Ltd is accurate and up to date.

5.7.2. Informing Assessment Services Ltd of any changes to information which they have provided, e.g. changes of address.

5.8. Sensitive information is only to be requested on a 'need to know' basis. This means only when the information is necessary to provide a service or support customers effectively.