Snap Operations Manual – 1. Snap Organisation & Management 1-12-1 Data Protection & Confidentiality Policy		
Prepared by: Angela Novell CEO MK Snap	**Issue Number:** 5	**Date of Issue: June 18**
Approved by: MK Snap Trust Board	**Signed:**	**Date:**

MK Snap DATA PROTECTION & CONFIDENTIALITY POLICY

MK Snap, as a provider of specialist services to young people and adults with special needs, collects and stores personal information on its learners for the purposes of delivering its services.

MK Snap will comply with the requirements of the Data Protection Act 1998, and register with the Public Register of Data Controllers via the Information Commissioners Office (ICO) for any data and images (including CCTV) held within scope.

This version of the Data Protection & Confidentiality Policy also takes into consideration the new General Data Protection Guidance (GDPR) that comes into force on 25th May 2018.

MK Snap will take all reasonable steps to maintain confidentiality of information, and ensure that electronic and paper records are securely maintained and stored. It is not MK Snap's practice to share confidential information with outside parties, however there are circumstances where confidentiality may be broken:

- Information and documentation relating to Service Users (Learners) funded within the scope of any local authority commissioning conditions of contract
- Where the person from whom the information was obtained and, if different, the person to whom it relates; consents
- Where the information is in the form of a summary or collection of information so presented that it is not possible to ascertain it relates to any particular individual
- When there is a serious risk of harm to the individual, as in a threatened suicide
- To protect others, for example, information about possible child abuse should be disclosed to the appropriate agency in line with the Safeguarding Policy
- To prevent a serious criminal act, especially where others may be endangered.
- To support the Police in the investigation of actual or alleged crime

Where a member of Snap staff has to break confidentiality, the person whose personal information it is, and their carer, will be informed that this is going to take place. MK Snap will take all reasonable steps to first encourage the individual and their carer to disclose the information voluntarily, and will obtain authority from the Chief Executive before disclosure actually takes place.

MK Snap will also have full regard for current and future legal requirements which may impinge on the confidentiality of personal information in general or specific categories of personal information e.g. rehabilitation of offenders.

Snap Operations Manual – 1. Snap Organisation & Management 1-12-1 Data Protection & Confidentiality Policy		
Prepared by: Angela Novell CEO MK Snap	**Issue Number:** 5	**Date of Issue: June 18**
Approved by: MK Snap Trust Board	**Signed:**	**Date:**

Principles

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

- Be obtained and processed fairly and lawfully,
- Be used only for the specified purposes for which it was obtained and not in any manner incompatible with those purposes,
- Be adequate, relevant and not excessive for those purposes,
- Be kept accurate and where necessary up to date,
- Not be kept longer than is necessary for those purposes,
- Be processed in accordance with individuals' rights under the Act,
- Be protected from unauthorised access, unlawful processing, accidental loss, destruction or damage,
- 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.

In relation to the new GDPR guidance the MK Snap Privacy Statement will be available on our website www.mksnap.org and will outline our commitment to ensure that we are GDPR compliant in the way that we approach data protection and our consideration of the new rights of the individual as follows:

- **The right to be Informed** as detailed in our privacy notice
- **The right of access** -within 30 days of a request we must be able to provide all information we hold on an individual
- **The right to rectification** - inaccurate or incomplete personal data must be rectified within 1 month of notification
- **The right to erasure/right to be forgotten** -individuals may request the deletion of personal data in some circumstances
- **The right to restrict processing** – individuals can restrict what we process we can hold data but not process it
- **The right to data portability** – an individual can ask for their data to be ported to another organisation
- **The right to object** - individuals can say no to us holding their data and we must give them that option
- **Right in relation to automated decision making and profiling** where potentially damaging decisions are made without human intervention

DEFINITIONS

- '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, volunteers, learners, individuals or organisations who come into contact with

the organisation eg: external contractors/partners. Information which can be classified as 'confidential' can broadly be grouped into the following areas:

- Information of a specific and personal nature about learner, employees or volunteers. If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others.
- Sensitive organisational information. This may be used to damage the organisation and other organisations, as well as individuals, staff or volunteers. It may be prejudicial to the business of the organisation or used to threaten the security of its property and systems.
- 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.

INFORMED CONSENT

- 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.
- 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.
- 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.
- 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.
- Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person.
- 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.
- Refusal to give consent should be respected wherever possible.

PASSING INFORMATION

When passing information to others, staff should:

- Check that the source of the request is bona fide;
- Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;
- Only send the information necessary for the purpose of the disclosure;
- Record exactly what has been passed on, to whom, when and why.

Snap Operations Manual – 1. Snap Organisation & Management 1-12-1 Data Protection & Confidentiality Policy		
Prepared by: Angela Novell CEO MK Snap	**Issue Number:** 5	**Date of Issue: June 18**
Approved by: MK Snap Trust Board	**Signed:**	**Date:**

DATA SECURITY

- The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:
- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.
- Documents containing individual data must not be left visible where it can be read by anyone inappropriately. This includes telephone messages, computer prints, letters and other documents.
- Electronic documents must be closed down when leaving a desk.
- All hardware containing data must be housed in a secure environment.
- All media containing staff information must be destroyed in a manner that ensures that data is not disclosed to an unauthorised person. Manual records should be shredded before disposal.
- Data should be password protected and the use of encrypted software employed to ensure that data is secure

SUBJECTS OF DATA

All individuals who are the subject of personal data held by MK Snap are entitled to:

- Ask what information the organisation holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the organisation is doing to comply with its obligations under the 1998 Data Protection Act.
- Their additional individual rights as detailed in the General Guidance on Data Protection GDPR from 25th May 2018

PRIVACY STATEMENT

From May 2018 MK Snap has issued a Privacy Statement which gives clear and transparent information to any data subject regarding how we use and store their data and a reminder of their rights under the new GDPR guidance. This will be available on the website from June 2018 and will be shared with all data subjects that MK Snap currently retain.

INTERNAL DATA PROTECTION AUDIT

MK Snap carries out an audit of data it holds on Learners, Supporters and Staff & volunteers. This is detailed in the document 1-12-2 MK Snap Internal Data Protection Audit. From May 2018 new approaches in line with GDPR requirements will be adopted to nominate a responsible person to complete regular audits of our compliance and to identify any data breaches. See the section on staff responsibilities.

1-12-1 Data Protection & Confidentiality Policy

Prepared by: Angela Novell CEO MK Snap	**Issue Number:** 5	**Date of Issue: June 18**
Approved by: MK Snap Trust Board	**Signed:**	**Date:**

RETENTION OF DOCUMENTATION

MK Snap will securely retain records of learners for a period not exceeding six years following the date from which the learner was no longer receiving services from MK Snap. A full list of retention timings can be reviewed as part of our audit procedures. All documents will be securely destroyed by shedding at the appropriate time, either internally, or by a specialist contractor. This includes electronic data storage for any data subject.

USE OF CCTV

MK Snap uses CCTV to monitor the security of its premises, and allows remote monitoring of its front doors when the reception area is not staffed. The CCTV system is accessible to the Chief Executive & Head of Support Services via their PC monitors. Images are stored for a period of seven calendar days, when they are then overwritten.

STAFF RESPONSIBILITIES

- **Angela Novell, Chief Executive** is responsible for monitoring the compliance of this policy within MK Snap, and where appropriate considering any revisions that may be relevant.
- **Caroline French, Head of Learner Services & Steve Carruthers** are responsible for ensuring all MK Snap staff understand their responsibilities in carrying out the policy, and considering situations that may lead to confidentiality being broken
- **Steph Passfield, Head of Support Services** is the responsible person for our audit and ensuring that we are able to identify any data breach
- **Matthew French, Marketing & Social Media Manager** is responsible for ensuring that our communications are appropriate and in line with policy guidance.
- **All other MK SNAP staff** are responsible for ensuring they understand the policy and how they apply it in their handling of confidential information and data.

POLICY REVIEW

This policy will be subject to annual review in light of any changes to legislation, or as a result of internal monitoring and audit. The policy will be reviewed and approved by the Board of Trustees.