Confidentiality, Data Protection and GDPR Policy

Purpose

To comply with Confidentiality, Data Protection Legislation and General Data Protection Regulations and guidance require SOS Homecare to use and share information in the provision of its services, as well as to protect the rights of individuals in respect of their personal details. One of the objectives of this policy is to reconcile the apparent conflict between the need to use (and share) information and the need to protect confidentiality. In the case of Service User information, whilst it is vital for the proper care of individuals that the professionals involved have ready access to the information they need, it is also essential that Service Users and their families are assured that their personal information will be kept confidential and that their privacy is respected. This policy establishes a basis for information sharing both within SOS Homecare Home/Services and offices, and between SOS Homecare and NHS, social service and non-NHS organisations.

Personal data includes information about any living individual that can be identified, such as Service Users, health professionals, other staff, and suppliers. The information may be held in manual or electronic form, and so includes, for example, the contents of filing cabinets, health care records, videos, test results and computer records.

Both the General Data Protection Regulations (GDPR) and the Caldicott recommendations are underpinned by sets of principles which are key both to gaining an understanding of the requirements and to interpreting these into working policies and procedures. This section details the principles and sets out their interpretations and policy implications.

Two key components of maintaining confidentiality are the integrity of information and its security. Integrity is achieved by safeguarding the accuracy and completeness of information through proper processing methods. Security measures are needed to protect information from a wide variety of threats.

Aims

- Observe conditions regarding the fair collection and use of information
- Meet legal obligations to specify the purposes for which information is used
- Collect and process appropriate information to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.

Scope

This policy applies to all staff

Introduction

The policy sets out the over-arching guidance and principles that flow from the Data Protection Act 1998, General Data Protection Regulations, the Caldicott Report recommendations, and the raft of other related legislation and central guidance which is used by NHS organisations. The latter form of guidance will be used in this policy as 'best practice'.

Key points for all SOS Homecare staff to follow are that:

a. Service users should be fully informed about how their information may be used.
b. There are strict conditions under which personal data may be disclosed.
c. In particular, certain disclosures are not allowed without express consent.
d. Individuals have the right to see what information is held about them, and to have any errors corrected.
e. Personal data should be kept secure and confidential at all times.
f. The legitimate use, disclosure or sharing of personal data does not constitute a breach of confidentiality. Sharing between organisations can take place with appropriate safeguards.
g. Sometimes a judgement has to be made about the balance between the duty of confidence and disclosure in the public interest. Any such disclosure must be justified.
i. Most of the requirements are common-sense precautions such as not divulging computer passwords, keeping manual records secure, and guarding against people seeking information by deception (for example, over the telephone).
j. Confidential and private information includes aspects such as not gossiping, improper use of information, e.g. taking care when discussing matters in public places. When it is necessary to discuss private and confidential matters in a public place it is not normally required to identify the Service User concerned.
j. If anyone is in doubt, they should refer to this and other policies and procedures, and if still in doubt ask their line manager, or the Organisation's Directors.

All staff should be aware of their responsibilities, and aware that a breach of security or infringement of confidentiality could lead to disciplinary action and even prosecution.

Responsibilities

All Staff

All staff within SOS Homecare are responsible for ensuring that:

- They comply with the requirements of GDPR (including the principles), and any SOS Homecare procedures and guidelines relating to data processing which may be issued from time to time.
- Any service user, staff or other individual's information they handle is as accurate and up to date as possible.
- Any personal information they provide to SOS Homecare in connection with their employment is accurate and up to date, e.g.: change of address. SOS Homecare cannot be held responsible for any errors unless the member of staff has informed SOS Homecare about the changes.
- Personal data is kept secure, relative to the security level of the data e.g. keeping the data locked in a filing cabinet drawer or room, ensuring that computerised data is password protected or kept only on disk which is itself kept securely.

- Personal data is not disclosed either orally, in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Training Manager
The training manager is responsible for ensuring new and existing employees receive training in confidentiality and data protection during their company induction and refresher training

Branch Manager
The Branch Manager is responsible for data compliance within their services, including training staff.

Finance Manager
The finance manager is responsible for compliance in relation to Finance data.

Directors
The directors have overall responsibility for GDPR, Confidentiality and Data Protection compliance for the company. The Managing Director is responsible for reporting data breaches to the Information Commissioner Officer as instructed in this policy.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct, which could ultimately lead to immediate dismissal.

Compliance with the principles of General Data Protection Regulations and Caldicott Report.

The GDPR
The principles of the GDPR apply to all staff handling personal information (on computer and manually held), and underpin all related policies and procedures. Article 5 of the GDPR requires that personal data shall be:

a) processed *lawfully, fairly* and in a *transparent* manner in relation to individuals;
b) collected for *specified, explicit and legitimate* purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) *adequate, relevant and limited* to what is necessary in relation to the purposes for which they are processed;
d) *accurate* and, where necessary, kept *up to date*; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for *no longer than is necessary* for the purposes for which the personal data are processed; personal data may be stored for longer periods where it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and
f) *processed* in a manner that ensures *appropriate security* of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, *compliance* with the principles."

Caldicott Report

The Caldicott principles and recommendations apply specifically to Service User-identifiable information and emphasise the need for controls over the availability of such information and access to it. In particular, the Managing Director has specific responsibilities to oversee an ongoing process of audit, improvement, and control in line with Caldicott Guardians.

The eight Caldicott principles, applying to the handling of Service User-identifiable information, are as follows

a. Justify the purpose for using confidential information
b. Use confidential information only when it is necessary
c. Use the minimum necessary confidential information
d. Access to confidential information should be on a strict need-to-know basis
e. Everyone with access to confidential information should be aware of their responsibilities.
f. Comply with the law.
g. The duty to share information for individual care is as important as the duty to protect patient confidentiality
h. Inform service users about how their confidential information is used

Processing

In relation to information or data, processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data.
- Retrieval, consultation or use of the information or data.
- Disclosure of the information or data by transmission, dissemination or otherwise making available,
- Alignment, combination, blocking, erasure or destruction of the information or data
- Viewing personal data, even where no changes are made to the data.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering a contract.
(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Informing and getting Consent

The general interpretation of the GDPR is that data subjects (Service Users, staff, etc.) need to be informed about how their information may be used and, in some circumstances, asked for their express consent.

In particular, a key implication, in conjunction with the Common Law requirement, is that individuals should be fully informed of the use to which information about them may be put and the extent to which it may be shared, and have the opportunity to make known any objections. In some circumstances this would convey the 'implied consent' of the individual.

If an individual (having been fully informed about the use of their information, including about the consequences, and having had the opportunity to object) wants information about themselves to be withheld from someone or some agency, the individual's wishes should be recorded and respected, unless there is a legal requirement to share this data.

Service user consent to disclosing

Service users generally have the right to object to the use and disclosure of confidential information that identifies them and need to be made aware of this right. Sometimes, if Service Users choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Service users must be informed if their decisions about disclosure have implications for the provision of care or treatment.

Where Service Users have been informed of:

a. The use and disclosure of their information associated with their healthcare, and
b. The choices that they have and the implications of choosing to limit how information may be used or shared;

then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that Service Users understand what may happen and are content should be taken.

Where the purpose is not directly concerned with the healthcare of a Service User however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

There are situations where consent cannot be obtained for the use or disclosure of Service User-identifiable information, yet the public good of this use outweighs issues of privacy. Appendix 1 of the Health and Social Care Act 2015 currently provides an interim power to ensure that Service User-identifiable information, needed to support a range of important work such as clinical audit, record validation and research, can be used without the consent of Service Users.

In branches that use EveryLife PASS, Service Users will provide consent to give their next of kin / relevant people access to OpenPASS. This will grant access to all documentation surrounding their care and will allow SOS Homecare to have a more holistic approach to care.

Consent Issues

Competence to consent

Seeking consent may be difficult, either because Service Users' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object).

a. Extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g., providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.
b. In the latter case, it will be important to check for a clear and unambiguous signal of what is desired by the Service User, and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

Failure to support those with disabilities could be an offence under the Disability Discrimination Act 1995 (and any subsequent amendments to this Act) and may prevent consent from being gained. Support for communicating with Service Users having specific disabilities can be obtained from a range of agencies, e.g.

a. Royal National Institute for the Blind
b. Royal National Institute for the Deaf
c. Disability Rights Commission – www.drc-gb.org
d. Speak ability – www.speakability.org.uk

Where Service Users are unable to give consent

If a Service User is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the Service User's best interests and any previously expressed wishes and be informed by the views of relatives or carers as to the likely wishes of the Service User. If a Service User has made his or her preferences about information disclosures known in advance, this should be respected.

Sometimes it may not be practicable to locate or contact an individual to gain consent. If this is well evidenced and documented and anonymised data is not suitable, the threshold for disclosure in the public interest may be lessened where the likelihood of detriment to the individual concerned is minimal. Where explicit consent cannot be gained and the public interest does not justify breaching confidentiality, then support would be needed under Appendix 1 of the Health and Social Care Act 2012.

Where the Service User is incapacitated and unable to consent, information should only be disclosed in the Service User's best interests, and then only as much information as is needed to support their care. This might, however, cause unnecessary suffering to the Service User's relatives, which could in turn cause distress to the Service User when he or she later learned of the situation. Each situation must be judged on its merits, and great care taken to avoid breaching confidentiality or creating difficulties for the Service User. Decisions to disclose and the justification for disclosing should be noted in the Service User's records. Focusing on the

future and care needs rather than past records will normally help avoid inappropriate disclosures.

Such circumstances will usually arise when a Service User has been unable to give informed consent to treatment, and, provided the Service User has not objected, this may justify the disclosure of some information with relatives in order to better understand the Service User's likely wishes. There may also be occasions where information needs to be shared with carers in order to assess the impact of disclosures to the Service User him or herself. Such occasions are rare and justifiable only in the best interests of the Service User.

Service users are often asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin'. It should be made clear that limited information will be shared with that person, provided the Service User does not object. This gives Service Users the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

Explicit consent

When seeking explicit consent from Service Users, the approach must be to provide:

a. Honest, clear, objective information about information uses and their choices – this information may be multi-layered, allowing Service Users to seek as much detail as they require.
b. An opportunity for Service Users to talk to someone they can trust and of whom they can ask questions.
c. Reasonable time (and privacy) to reach decisions.
d. Support and explanations about any form that they may be required to sign.
e. A choice as to whether to be contacted in the future about further uses, and how such contacts should be made.
f. Evidence that consent has been given, either by noting this within a Service User's health record or by including a consent form signed by the Service User.

The information provided must cover:

a. A basic explanation of what information is recorded and why, and what further uses may be made of it.
b. A description of the benefits that may result from the proposed use or disclosure of the information.
c. How the information and its future uses will be protected and assured, including how long the information is likely to be retained, and under what circumstances it will be destroyed.
d. Any outcomes, implications, or risks, if consent is withheld (this must be honest, clear, and objective – it must not be or appear to be coercive in any way).
e. An explanation that any consent can be withdrawn in the future (including any difficulties in withdrawing information that has already been shared).

The information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences.

The right to withhold or withdraw consent

Service users do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare. Where Service Users are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a Service User exercising his or her right to refuse treatment.

There are a number of things to consider if this circumstance arises:

a. The concerns of the Service User must be clearly established, and attempts made to establish whether there is a technical or procedural way of satisfying the concerns without unduly compromising care.
b. The options for providing an alternative form of care or to provide care through alternative arrangements must be explored.
c. Decisions about the options that might be offered to the Service User have to balance the risks, staff time and other costs attached to each alternative that might be offered against the risk to the Service User of not providing healthcare.

Every effort must be made to find a satisfactory solution. The development of technical measures that support Service User choice is a key element of work to determine the standards for electronic integrated care records. Careful documentation of the decision-making process and the choices made by the Service User must be included within the Service User's record.

Sensitive Personal (Special Category) Data

SOS Homecare may from time to time process "sensitive personal data" relating to staff, service users and other individuals. For example, data relating to the ethnic origin of individuals may be processed for the purposes of equal opportunities monitoring or to identify any necessary dietary requirements. Medical records need to be processed for the provision of healthcare and general welfare, to identify any necessary dietary and accommodation requirements and to assist in meeting the needs of individuals with disabilities. In exceptional circumstances, SOS Homecare may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

In context to the above, where sensitive personal data are to be held or processed, SOS Homecare will normally seek the explicit consent of the individual in question, unless one of the limited exemptions provided in the GDPR applies, (i.e.: to perform a legal duty regarding employees, or to protect the data subjects, or a third party's vital interests).

Maintaining health care records

Service users' records should be factual, consistent and accurate:

a. Be written (on paper or electronically), as soon as possible after an event has occurred, providing current information on the care and condition of the Service User.
b. Be written (on paper or electronically), clearly, legibly and in such a manner that they cannot be erased.

c. Be written (on paper or electronically), in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly.
d. Be accurately dated, timed and signed, or otherwise identified, with the name of the author being printed alongside the first entry. Be consecutive and ensure documentation is in chronological order
e. Be readable on any photocopies.
f. Be written (on paper or electronically), wherever applicable, with the involvement of the Service User or carer.
g. Be clear, unambiguous, (preferably concise) and written (on paper or electronically), in terms that the Service User can understand. Abbreviations, if used, should follow common SOS Homecare conventions.
h. Be written (on paper or electronically), to be compliant with the Race Relations Act and the Disability Discrimination Act.

Service user records should be relevant and useful:

a. Identify problems that have arisen, and the action taken to rectify them.
b. Provide evidence of the care planned, the decisions made, the care delivered, and the information shared.
c. Provide evidence of actions agreed with the Service User (including consent to treatment and/or consent to disclose information).

Service user records should include

a. Medical observations: examinations, tests, diagnoses, prognoses, prescriptions and other treatments.
b. Relevant disclosures by the Service User – pertinent to understanding cause or effecting cure/treatment.
c. Facts presented to the Service User.
d. Correspondence from the Service User or other parties.

Service user records should not include

a. Unnecessary abbreviations or jargon.
b. Meaningless phrases, irrelevant speculation or offensive subjective statements.
c. Irrelevant personal opinions regarding the Service User.

Keeping Service User information physically and electronically secure

Staff should not leave portable computers, medical notes or files in unattended cars or in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used. Staff should not normally remove health care records from the Home/Service, and where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed. All electronic devices should be password protected and passwords must not be shared with anyone other than the user.

Documentation should not be screen shotted or downloaded onto personal devices.

Keeping Service Users' information secure

The security principle within the GDPR goes beyond the way we store or transmit information. Every aspect of our processing of personal data is covered, not just cybersecurity.
The security measures we have put in place seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those authorised to do so (and that those people only act within the scope of the authority we have given them);
- the data we hold is accurate and complete in relation to the reason for processing it;
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, we have systems in place to recover it and therefore prevent any damage or distress to the individuals concerned.

<u>For all types of records, staff working in offices where records may be seen must:</u>

a. Shut/lock doors and cabinets as required.
b. Wear building passes/ID if issued.
c. Query the status of strangers.
d. Know who to tell if anything suspicious or worrying is noted.
e. Not tell unauthorised personnel how the security systems operate.
f. Not breach security themselves.

<u>Manual records must be:</u>

a. Returned to the filing location as soon as possible after use.
b. Stored securely within the office, arranged so that the record can be found easily if needed urgently.
c. Stored closed when not in use so that contents are not seen accidentally.
d. Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
e. Held in secure storage with clear labelling. The availability of secure means of destruction, e.g. shredding, are essential.

<u>With electronic records, staff must:</u>

a. Always log-out of any computer system or application when work on it is finished.
b. Not leave a terminal unattended.
c. Not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
d. Not reveal passwords to others.
e. Change passwords if there is a possibility that it may have been compromised.
f. Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children's or pet's names or birthdays).
g. Always clear the screen of previous Service User's information before seeing another.
h. Use a password-protected screen-saver to prevent casual viewing of Service User information by others.
i. Use password protected documents when sending out rotas.

Common Law and disclosure in the Public Interest

The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form, except as originally understood by the confider, or with his or her subsequent permission.

There are exceptions to the duty of confidence that may make the use or disclosure of confidential information appropriate. Statute law requires or permits the disclosure of confidential Service User information in certain circumstances, and the Courts may also order disclosures. Case law has also established that confidentiality can be breached where there is an overriding public interest.

Examples of disclosure to protect the public would be the risk of a serious crime occurring, national security or the risk of serious harm.

Human Rights Act 1998

Article 8 of the European Convention on Human Rights, which is given effect in UK law by the Human Rights Act, establishes a right to 'respect for private and family life'. This may be open to some interpretation in points of detail by the courts in years to come, but it creates a general requirement to protect the privacy of individuals and preserve the confidentiality of their health records. It underpins the Confidentiality Model presented in this code of practice. There are also more general requirements in relation to actions having legitimate aims and being proportionate to the need. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

SUBJECT REQUESTS

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request (to exercise any of the above rights) verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point.

A request does not have to refer to the specific right, or the GDPR, as long as it is clear that the individual is making a request relating to their own personal data.

Timescales & fees

We must act on the subject requests without undue delay and at the latest within one calendar month of receipt of the request. The time limit is calculated from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

In most cases we cannot charge a fee to comply with subject requests. However, where the request is unfounded or excessive, we may charge a "reasonable fee" for the administrative costs of complying with the request. We may also charge a reasonable fee if an individual requests further copies of their data following a request. The fee will be based on the administrative costs of providing further copies.

The Freedom of Information Act 2000 gives individuals extended rights of access in certain circumstances to information which is not held on computer or in a relevant filing system. Please contact the relevant Manager for further information.

Retention of Data
SOS Homecare will hold information for differing lengths of time, depending on legal and operational requirements, following which they will be destroyed. This will be done in accordance with the retention periods detailed in the SOS Record Keeping, Retention and Archiving Policy being compliant with the Act.

E-mail
It is permissible and appropriate for SOS Homecare to keep appropriate records of internal communications, provided such records comply with the GDPR principles.

However, all SOS Homecare staff need to be aware that:
- The Act applies to e-mails which contain personal data about individuals which are sent or received by SOS Homecare staff.
- Subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to e-mails which contain personal data concerning them, provided that the individual data subjects can provide sufficient information for SOS Homecare to locate the personal data in the e-mails.
- The legislation applies to all e-mails from and to SOS Homecare staff which are sent and received for business purposes.
- E-mails, like other correspondence, need to be managed and archived for as long as necessary in order to meet local and corporate business needs.

Reporting of Data Breaches
The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

We will ensure that we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not any data breach needs to be reported.

We will keep a record of any personal data breaches, including those which do not require reporting.

If a data breach occurs, please refer to the Data Breach Reporting Flow Chart (Appendix 1).

Notification to the Information Commissioner
SOS Homecare has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Notification submission will be

completed by the Branch Manager or more senior manager. Notification monitoring within SOS Homecare is carried out by the company directors. Individual data subjects can obtain full details of SOS Homecare's data protection registration/notification with the Information Commissioner or from the Information Commissioner's website (https://ico.org.uk).

Training

It is therefore vital that our staff:

- understand the importance of protecting personal data,
- are familiar with this policy, and
- put its procedures into practice.

All staff will receive appropriate initial and refresher training bi-ennially, including:

- our responsibilities as a data controller under the GDPR;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions we place on the personal use of our systems by staff (e.g. to avoid virus infection or spam).

Cyber Security

Increasingly data is stored and transferred digitally. It is therefore important for the company to take appropriate steps to ensure that IT systems are secure. SOS Homecare is committed to following the 5 technical controls outlined in the Cyber Essentials self-help guide:

- Use a firewall to secure internet connections
- Choose the most secure settings for devices and software
- Control who has access to data
- Protect IT systems against viruses and other malware
- Keep devices and software up-to-date

Passwords

Passwords will be issued to staff when they commence employment with the company. Staff should not change their password and they do not need to write it down – the System Administrators have a record of passwords issued. This list is stored securely but can be accessed easily by a System Administrator should staff forget their password.

If staff believe that their password may have been compromised they must inform their line manager immediately, who will make arrangements for a new password to be issued by one of the System Administrators. The line manager will also ensure that no further data breach has occurred.

Passwords will take the following format

- Email Accounts - 11 characters - Mixture of lower case, upper case, numbers and special characters
- Care Planner – minimum 8 characters – mixture of lower case, upper case, numbers and special characters
- Laptops/Desktop – 5 digit pin number or password
- Everylife PASS - At least eight characters, can’t contain the username or the word 'password', must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols

For financial systems, a process of 2-factor authentication will be required.

Review
This policy will be reviewed annually.

Appendix 1

Data Breach Reporting Flowchart