Information Governance and Security Policy Manual

Revision 0.3

Revision History

The document is issued as a draft form, starting at Revision 0.1. After reviews, any further document updates will increase the revision number to 0.2, 0.3 etc. Once the document is approved, revision number will change to 1.0.
This document will be reviewed periodically and will be amended as and when needed to reflect the latest modifications and/or upgrades. Details of each amendment will be entered into the amendment record below and revision will change to 1.1, 1.2 1.3 etc, until the document gets approved and document version will change to 2.0 (X.0 for the future iterations).

Revision	Date	Author	Title	Changes
0.1	01/06/2019	Rupert Stocks	Data Protection Officer	New document
0.2	01/06/2019	Rupert Stocks	Data Protection Officer	Minor grammatical changes
0.3	05/03/2020	Rupert Stocks	Data Protection Officer	Additional access control – firewalls and MFA update

Approval

By signing and dating in the space provided below, the below company representatives indicate approval of this document.

Each document should be reviewed at least by one independent reviewer and one quality assurance reviewer; where applicable, other managers may need to approve the document.

Reviewed and Approved by:	Name	Signature/Email approval	Date
Data Protection Officer	Rupert Stocks	email	
Caldicott Guardian	Adam Waterhouse	email	
SIRO (Board member)	Tuvi Orbach	email	

Contents

Introduction

1.1 Purpose

This document is the policy manual for information governance and information security management in MindLife. Through a comprehensive suite of information governance objectives, security control objectives and supporting policy statements, this manual explains how the NHS IG Toolkit and ISO 27001, the international standard code of practice for information security management, applies within MindLife. Its purpose is to communicate management directives and standards of care to ensure consistent and appropriate protection of information throughout MindLife.

This policy has been designed to provide a framework of control and safeguards for the governance and security of the information and systems used within MindLife Ltd. Where MindLife Ltd is connected to the HSCN network, then this policy is in addition to the requirements specified within the HSCN Connection Agreement.

It is important that MindLife has a Governance Framework and information security policy to provide management direction and support on matters of information security and confidentiality. Information systems form a major part of the efficiency of the organisation. Adequate security procedures are critical in ensuring the confidentiality, integrity and availability of these systems and their associated data. Information Security concerns everyone in MindLife Ltd. All members of staff and contractors have a responsibility to ensure it is maintained.

Wherever personal information is held on paper or computer, it is subject to the principles of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Individuals and the business may be prosecuted or subject to a claim for damages for any instance where the data protection principles are breached or where a person suffers loss, damage or harm from misuse of information.

Applying this policy to normal working within MindLife Ltd is therefore mandatory for all members of staff/contractors and will greatly reduce the risk of loss, damage or misuse of information. Staff/Contractors must be be aware that non-compliance may result in disciplinary action being taken against the individual and may result in termination of employment or contract and/or legal action.

1.2 Scope

This document applies to all information/data, information processing/computer systems and networks (collectively known as “information assets”) owned by MindLife Ltd, or those entrusted to MindLife Ltd by third parties, including and not limited to project documents, medical reports and patient records.

This document provides useful information and recommendations to the following individuals:

- Employees/Contractors: All MindLife employees (including managers, staff, temporary employees in all areas including IT, Admin, etc) and third parties (such as consultants, contractors, support/maintenance staff) acting in a similar capacity.

- Other third parties: such as business partners, external auditors and industry regulators.

1.3 Document Change Control

Since it incorporates formal statements of MindLife Ltd policy, this manual is subject to a change control process following MindLife document control procedure.

1.4 Definitions and Acronyms

Definition / Acronym	Description

Access, access rights	Ability of a user or program to interact with an information asset e.g. to read or write data, send messages over the network etc.; also ability of a person to enter a site, building, room, wiring closet etc.
Access control	Type of control designed to restrict access to an information asset. Permitting authorised access while preventing unauthorised access. "Means to ensure that access to assets is authorised and restricted, based on business and security requirements" (ISO/IEC 27000).
Accident	Although we tend to think that security incidents result from Deliberate acts by hackers, malware etc. but most are in fact the result of chance events, errors and mistakes.
Accountable, accountability	A person who is held accountable for something is personally responsible for it and may be disciplined if they do not fulfil their obligations. Unlike responsibility, however, accountability is similar To ownership in that it cannot be delegated to another.
IT	Information Technology
HSCN	The National Health Service Intranet
Personal Data	**I**nformation that relates to an identified or identifiable individual.
Special Category Data	Special category data is personal data that needs more protection because it is of a more sensitive nature such as health records

1.5 References

#	Document
1	ISO 27001
2	ISO 27002
3	ISO14971
4	ISO 13485
5	The Data Protection Act / GDPR
6	MindLife Confidentiality Agreement
7	Caldicott sharing of personal information
8	NHS Data Security and Protection Toolkit

1.6 Emergency Policy Exceptions

Where justified and necessary under exceptional circumstances, limited policy exceptions may be made without prior management approval. Where prior notification and acceptance of policy exceptions is not possible (for example in an emergency), exceptions must however be reported to the management as soon as possible thereafter (within a few working days at most). By definition, emergency exceptions are not anticipated to be routine in nature.

2 Overview

This process document is based on ISO 27001 and the NHS Data Security and Protection Toolkit. The process is explicitly concerned with information security, meaning the security of information assets in MindLife, and not just IT/systems security. The IT department is merely the custodian of a good proportion of the organisation's information assets and is commonly charged with securing them by the information asset owners.

3 Information Governance Management Framework

This document covers the framework, policy and procedures for information governance and security. The MindLife CEO and management team are committed to supporting the aims of this document.

3.1 Senior Roles and Governance Body

MindLife have an Information Management and Security Group which meet formally once a year. The group consists of the Senior Information Risk Owner (SIRO), the Data Protection Officer and the Caldicott Guardian. Other MindLife employees or contractors may attend the meeting on an ad-hoc basis to present a report or provide an update on a specific matter. The group is responsible for supporting, improving and evolving the Information Governance Agenda. Additionally information governance and security is a standing agenda item on management meetings and any immediate issues relevant to IG and security are discussed and actioned at this meeting.

3.2 Key Policies

This document covers IG Policy, Security Policy, the Data Protection Act/GDPR responsibilities, requirements for staff training and incident management.

4 External Parties

Information security is not to be compromised by the introduction of third party products or services. Risks must be assessed and mitigated when dealing with customers and in third party agreements. A third party agreement template is included in the appendices of this document.

5 Asset Management

MindLife maintains a record of the information assets it holds, and manages their security appropriately.

IT assets include not only hardware and software but also business and service user data. Identifying and classifying IT assets, and allocating ownership/custodianship responsibilities is the first step towards applying appropriate protective controls.

5.1 Responsibility for Assets

All information assets should be accounted for and have a nominated owner. Information assets that contain patient data must be accounted for and have a nominated owner. This inventory must record a description, ownership and location of the assets, the type of protection employed to secure the asset and what type of information is recorded. MindLife maintain personal and confidential information within a secure cloud network environment but it is recognised that from time to time some of this information might be temporarily downloaded onto other assets or stored in hardcopy form. When this occurs this policy applies to all those devices and locations.

5.2 Information Classification

Printed information of a sensitive nature such as patient identifiable data must be labelled as confidential, protected from unauthorised access or viewing and when not in use stored in a secure location. The only permanent location patient identifiable data records will be stored electronically is the MindLife secure cloud server network. This will have restricted access to authorised personnel only. Electronic information of a sensitive business nature should be stored with restricted access on MindLife business servers and devices.

6 Human Resources Security

MindLife manages system access rights etc. for ‘joiners, movers and leavers’, and must undertake suitable security awareness, training and educational activities as part of staff/contractor induction processes and ongoing training.

The department managers are responsible to implement and verify the following;

6.1 Prior to employment

Security responsibilities must be taken into account when recruiting permanent employees, contractors and temporary staff (e.g. through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements on security roles and responsibilities).

6.1.1 Roles and responsibilities

Security roles and responsibilities including compliance with this Information Governance and Security Manual as well as any specific responsibilities for the protection of particular information assets or for the execution of particular security processes or activities (such as reporting security incidents or near misses), will be documented where appropriate for example in job descriptions, employment contracts and consultancy agreements.

Job descriptions and so forth will be maintained and updated to reflect changes in roles and responsibilities, particularly in respect of information security aspects. At the very least, job descriptions etc. will be reviewed by an employee's manager at the time of the annual appraisal or whenever someone is promoted.

6.1.2 Screening

All potential recruits (including permanent employees, consultants, contractors and temporary staff will be adequately screened prior to being offered employment, especially in the case of applicants for particularly sensitive or responsible positions where the candidate's integrity (honesty and trustworthiness) and competence (skills, experience and qualifications) are vital. The screening process cannot absolutely guarantee a candidate's integrity or competence but is a means to reduce the risk of employing unsuitable people. The extent of screening will therefore reflect the risk associated with abuse of the position. Where permitted by local law, pre-employment screening for all applicants should include the following checks:

Assessing the completeness and accuracy of the applicant's *curriculum vitae* (including academic and professional history and qualifications) by discussion with the applicant at interview and/or by other means;

Checking the identity of the applicant, in line with the company recruitment policy.

Availability of satisfactory character references.

Additional checks might be performed if a candidate is anticipated to need significant access to special category information, such as:

Criminal record and/or other background or security checks (the candidate's explicit permission is normally required for checks of this nature).

Such additional checks may be repeated periodically for workers holding positions of considerable authority, or where there are valid reasons for management to doubt their integrity or competence.

Where workers are provided through an agency, the contract with the agency must clearly specify the agency's responsibilities for screening and the notification procedures they must follow if screening has not been completed or if the results give cause for doubt or concern. MindLife must periodically confirm the agency's compliance with these requirements, and be alert for non-compliance (*e.g.* unsuitable candidates being placed).

Management must evaluate the need to supervise new and inexperienced workers with access to significant information assets including sensitive information. The work of all workers must be periodically reviewed and approved by managers or other senior or trusted employees.

Managers should be aware that personal circumstances of their staff may affect their work. Personal or financial problems, changes in their behaviour or lifestyle, recurring absences and evidence of stress or depression might lead to fraud, theft, error or other security implications. Fraudsters sometimes betray their activities by 'conspicuous consumption' or 'living beyond their means'. Suspicions of this nature should be reported to Human Resources.

Personal information about candidates must be regarded as confidential and protected accordingly.

6.1.3 Terms and Conditions of Employment

The terms and conditions of employment (whether included directly in employment or similar contracts, or referenced in external documents such as the Code of Conduct must clearly state the worker's obligation to comply with MindLife's information governance and security policies. The intention to initiate disciplinary actions if an employee disregards their security obligations must be noted unambiguously.

The worker's obligations and rights regarding Copyright, Data Protection and other applicable laws must also be clearly stated. Responsibility for the classification, handling and management of the employer's information should also be included. If appropriate, terms and conditions of employment must state that these responsibilities extend beyond MindLife's premises, outside normal working hours (e.g. home or teleworking) and may persist after employment ceases.

Workers must sign to denote their understanding and explicit acceptance of the terms and conditions of employment prior to being permitted access to MindLife's information assets.

All new employees will receive a copy of this policy from HR as part of their induction and will be required to sign the record before taking up their duties.

6.2 During Employment

Management responsibilities regarding information security should be defined. Employees and (if relevant) third party IT users should be made aware, educated and trained in security procedures. A formal disciplinary process is necessary to handle security breaches.

Employees must be made aware of and motivated to comply with their obligations under these information security policies plus the associated standards, procedures, guidelines, laws and regulations.

6.2.1 Management Responsibilities

All workers must comply with MindLife's information security policies, standards, procedures and guidelines, plus requirements identified in the terms and conditions of their employment or service contracts and applicable laws and regulations.

Managers are responsible for ensuring that, throughout their employment, workers:

- Are properly briefed and made aware of their security responsibilities before being granted access to MindLife networks, systems or data, and periodically thereafter;
- Are motivated to comply with their responsibilities through a combination of ongoing management supervision, encouragement and reinforcement;
- Maintain their information security competencies, skills and qualifications through ongoing awareness, education and training.

6.2.2 Staff Responsibilities

- All members of staff and contractors are required to preserve the security of the assets and information of the business and bring any concerns that threaten this security to the attention of the MindLife Caldicott guardian.
- Each member of staff must be aware of his/her responsibilities when using information that is personal and be aware that it may only be used in accordance with the Data Protection Act 2018 and GDPR.
- Each member of staff must be aware of the responsibilities and know how to contact the key post holders for Information Governance within MindLife. These are the Data Protection Officer and the Caldicott Guardian.
- Staff/Contractors must also be aware that clinical information within MindLife Ltd is governed by the Common Law Duty of Confidentiality and Caldicott good practice principles.
- All members of staff and contractors are required to read and familiarise themselves with the rules and procedures contained in this policy. Compliance is compulsory for **ALL**.
- All existing staff and contractors with access to confidential and personal records are required to sign the Information Governance and Security Policy Communication Record, which is held by the HR department, to confirm they have read and understood it – see Appendix. HR will ensure that current employees sign the record.
- All staff and contractors with access to personal and confidential data must carry out the requirements that are defined in the NHS Data Security and Protection Toolkit according to their role within the company.

6.2.3 Data Protection Officer.

The role of the Data Protection Officer is to develop IG policy, coordinate, publicise and monitor the standards of information handling throughout MindLife Ltd, ensuring that employees are fully informed of their own responsibilities for maintaining the standards set.

Responsibilities

- The Data Protection Officer along with the senior management within MindLife will maintain and develop effective IG policies and procedures
- The Data Protection Officer will ensure that every member of staff, including staff and contractors who may only visit on a casual basis but require access to information or computer systems necessary to carry out their role, understands the principles within this policy.
- The Data Protection Officer will co-ordinate the training and development of staff to use the information systems in accordance with the necessary guidance and relevant legislation.
- The Data Protection Officer will provide a focal point for the resolution and discussion of IG and security issues.

6.2.4 Caldicott Guardian

A key part of the recommendations contained within the Caldicott report was the establishment of a network of Caldicott Guardians of patient information; MindLife Ltd has a nominated Guardian. The Caldicott Guardian acts as a conscience in matters of data confidentiality and sharing. They work as

part of a broader Information Governance function within MindLife Ltd.

Responsibilities

- The Caldicott Guardian has responsibility to develop a framework of protocols to safeguard and govern the uses made of patient information within the MindLife organisation.
- The Caldicott guardian should ensure the compliance within the NHS code of practice and that staff are aware of their individual responsibilities through policy, procedure and training.
- The Caldicott guardian ensures that appropriate mechanisms are in place to obtain patient informed consent in the collection, processing and sending of their personal data.
- The Caldicott guardian will be responsible for the monitoring and auditing of access to confidential personal information.
- The Caldicott guardian will be responsible for and maintain a log of all significant information security breaches and events.

6.2.5 Information Security Officer (ISO)

The role will develop, implement and support Information Security measures within MindLife Ltd, maintaining and updating the security measures outlined in the Information Governance Toolkit and other measures of Information Security as required, including compliance with ISO 27001 and staff management responsibilities.

Responsibilities

- The ISO will ensure compliance with the information security components of the Data Security and Protection Toolkit
- The ISO will ensure security considerations of information systems are in line with MindLife's approved definition of risk
- The ISO will ensure all arrangements for managing information security are effective and aligned with with MindLife's Information security and risk policies
- The ISO will assist in the development of the business continuity management arrangements for key information assets
- The ISO will provide advice and guidance regarding the implementation of controls to mitigate against malicious or unauthorised code
- The ISO will assist in designing and configuring access controls for key systems.

6.2.6 Information Security Awareness, education and training

All workers should receive appropriate training and regular updates in information security policies, standards, procedures, laws, regulations etc. where relevant to their job functions. This includes security requirements, legal responsibilities and business controls (such as security incident reporting processes), as well as induction training in the appropriate and secure use of IT facilities before access to information or IT services is granted. Security awareness, education and training activities should reflect workers' needs e.g:

Managers should receive information on their information security management, supervisory and governance responsibilities.

IT professionals, whether or not they are employed within the IT function itself, should be informed about the technical aspects of information security.

Workers who routinely handle sensitive and valuable proprietary or personal data should be reminded periodically of their confidentiality and integrity obligations.

Workers must be aware that access to person identifiable data will be monitored and confidentiality audits will be carried out by the MindLife's Data protection officer.

All workers should be briefed about information security in general terms.

6.2.7 Disciplinary process

Workers who commit a security breach (for example deliberately violating these information security policies or related security standards, procedures, guidelines, laws or regulations) should be disciplined through the standard disciplinary process owned by Human Resources, or (in the case of non-employees and contractors) through contractual or legal processes.

All workers must be treated fairly and correctly, based on reliable evidence verifying that breaches have occurred. The disciplinary process allows for a range of actions according to the severity of the violation, potentially including summary dismissal and legal action to recover losses and consequential damages. Workers who break the law may also be prosecuted.

Where appropriate and provided that any confidentiality issues are taken into account, uses and outcomes of the disciplinary process should be communicated among managers and peers to reinforce MindLife's policies in this area.

6.3 Termination or change of employment

Security aspects of a person's exit from the organisation (*e.g*. the return of corporate assets and removal of access rights) or change of responsibilities should be managed.

A worker's exit from or change of status within, the organisation must be properly managed and controlled such that information assets are retrieved and information access rights are promptly revoked where no longer justified.

6.4 Termination responsibilities

Managers are responsible for ensuring that suitable termination processes are completed when subordinate workers leave MindLife:

Standard termination checklists must be completed and returned to departmental heads.
Workers must be reminded of their ongoing legal and ethical responsibilities to maintain the confidentiality of proprietary and personal information obtained in the course of their employment.

Similar considerations apply when a worker transfers between departments or changes status within MindLife. The managers involved in a transfer should jointly agree a fixed transition period, beyond which the worker will no longer have access to information and other assets exclusively associated with their previous role. It is particularly important that key controls relating to divisions of responsibility is not compromised at this time *e.g*. the worker should not be able to initiate a payment under the old role and approve it under the new role.

6.5 Return of assets

Workers must return all MindLife assets (including documents, data, computer systems, mobile phones, corporate credit cards, access tokens and authentication devices *etc*.) in their possession when they leave MindLife. Managers should explicitly request this, for example in the course of completing the termination checklist.

Workers with vital knowledge should be encouraged to 'hand-over' to their peers before they leave, ideally by preparing procedures and other notes [this process should be happening routinely in any case to minimize reliance on critical people].

6.6 Removal of access rights

Workers' access to information, computer/network systems and facilities must be revoked promptly when they leave MindLife, or revised if they transfer or change status. This includes logical and physical access rights *e.g*. userIDs and passwords (including any shared userIDs and group access rights), authentication tokens, access cards, keys *etc*. Responsibility for achieving this are the workers managers.

In circumstances such as summary dismissal for fraud or theft, the risks relating to a worker's termination may justify the immediate revocation of their access rights. In conjunction with Human Resources, the employees manager should ensure that the risks of continued access are assessed and appropriate action is initiated at the earliest opportunity (*e.g*. immediate revocation of the worker's network login ID). In such cases, there may also be a need to retain logs and other files and information for forensic analysis. General physical access methods such as number pad entry systems should also be considered.

7 Physical and environmental security

Valuable IT equipment should be physically protected against malicious or accidental damage or loss, overheating, loss of mains power etc. Physical security is obviously an important issue for a data centre but is also important for network switches, desktop workstations, portables and handheld devices, and in fact all locations where MindLife workers work.

7.1 Secure areas

Access by key code is required to access the MindLife offices. Additional security such as lockable filing cabinets should be used for personal data such as patient consent forms, personnel records etc. Guests are signed in and out of the premises and not left unsupervised within the office premises.

7.2 Equipment security

Critical IT equipment, cabling and so on should be protected against physical damage, fire, flood, theft etc., both on- and off-site. Power supplies and cabling should be secured. IT equipment should be maintained properly and disposed of securely.

8 Communications and operations management

Systems and network managers normally require powerful access rights in order to do their jobs, implying a very high degree of trust. IT operations professionals have privileged access to our systems and networks against their trustworthiness and competence, and cover several other aspects of systems/network management that directly influence information security (e.g. data backup and change control procedures).

8.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Duties should be segregated between different people and functions where possible (*e.g*. access to development and operational systems should be segregated).

8.2 Third party service delivery management

Security requirements should be taken into account in third party service delivery (*e.g*. IT facilities management or outsourcing), from contractual terms to ongoing monitoring and change management.

8.3 Back-up storage and retrieval

Backup and storage should also be compliance with this policy and part of the MindLife Backup and Retrieval policy.

8.4 Network security management

Network management and access should be controlled by IT department and approved by designated IT manager.

Patient identifiable data must follow extra security measures and stored within the MindLife secure network. This network is kept as a separate and isolated network accessible only by authorised individuals using two factor authentication over a secure VPN connection. Subsequent access to the MindLife platform and patient database is controlled by additional username/password restrictions. Users of the system are further restricted to only being able to access the parts of the platform granted to them by nature of their role. The MindLife Information security officer is responsible for maintaining a list of authorised users to the MindLife network and platform and for granting and revoking access rights.

Staff given authorisation to access patient data need to be approved by MindLife senior managmement. All access to the MindLife platform containing patient identifiable records is recorded by the sytem in an audit log providing full traceability.

As part of MindLife security policy in the office and safeguarding patient data in the computers, all.password that can access patient data should be

- a minimum length of 10 characters without requiring a mix of character types;
- not matching your previous four passwords;
- not detected as a common password, e.g. password1234; and
- not detected as a breached password (a password used for an account that has previously been compromised)

8.4.1 Threat of malicious software

MindLife shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Only properly licensed software from reputable sources will be used on MindLife computing equipment. Critical systems will be regularly backed up such that it is possible revert to a virus free state following an infection. All office PC's, laptops and Files Servers are protected by Anti-Virus Software.

The Information Security Officer is responsible for ensuring that:

- Anti-virus software has been deployed and configured for the real time detection and reporting of viruses on all networked workstations, servers and electronic mail.
- Updates are applied on a regular basis..
- Systems are virus checked following system up-grades, maintenance and prior to commissioning systems for operational use.
- The Information asset register contains information on the method of protection for all information assets.

All users should:

Be on the alert for unsolicited or suspicious emails, files or software.

Promptly report actual or suspected virus infections to the Information Security Officer. In event that there is a virus infection the equipment concerned must be switched off and disconnected from the network. It should then be labelled 'Not for use' and it should not be re-used until the Information Security officer has investigated and taken any action necessary to ensure the equipment is free from infection.

Not install software or change the configuration of equipment unless authorised to do so.

Not install games, screensavers or other software not required for genuine business reasons.

Never disable, alter the configuration or remove anti-virus software.

.

8.4.2 Storing personal information

Any electronic file that contains patient identifiable data should be stored on the MindLife secure cloud network. The exception to this is incident reports or related documentation that might contain some person identifiable data. These reports are stored with restricted user rights or if in paper format within locked filing cabinets and are under the control of the MindLife Caldicott Guardian.

Any sensitive business data is stored in restricted user rights folders on the main business system.

Network users who work with such information must be informed about the sensitivity of the subject and must be trained how use and store the data safely.

8.4.3 Use of the NHS number

The key purpose of using the NHS number is to improve patient safety. The NHS number must be present in all active patient records and determined as early as possible in each episode of care. The NHS number is the only national unique patient identifier in operation in the NHS, and its comprehensive use is fundamental to improving patient safety and confidentiality across all care settings.

All patient records within the MindLife systems must have the ability to record the NHS number. MindLife recognise the difficulty of obtaining the NHS number in all cases but the option to enter the number should be present. The NHS number (if present in the record) should be used as a key field in all transfer processes such as patient letters, GP letters or electronic transfers.

8.4.4 NHS National Opt Out

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes. This applies to all personal and confidential information supplied by the patient that has not been anonymised.

MindLife will ensure that technical solutions exist to comply with the National opt out requirements if any confidential patient information is to be used beyond an individual's patient care and has not been anonymised for such purposes.

8.4.5 Emailing personal information

Employees/Contractors must be educated and trained in relation to the risks of emailing personal information. Patient identifiable data must never be emailed except by using the secure email transfer facility provided by NHS mail network (NHS.net) or by approved cryptographic controls (currently AES 256 bit strength or equivalent).

8.4.6 Posting personal information

Personal data required as a hardcopy should be sent by first class post in a non-windowed envelope, marked 'Private and Confidential' with the intended recipient clearly indicated. In some cases recorded post should be considered. The sending of multiple records via post should be discouraged but if required must be via a secure courier service.

8.4.7 Storing hard copies information

Any hard copy document that contains personal information including person identifiable data such as patient consent forms must be in held in storage that requires an entry key or other suitable security measure. Only authorised people have access to these keys.

8.4.8 Anonymising personal Information

It is a legal requirement that when patient data is used for purposes not involving the direct care of the patient, i.e. secondary use the patient should not be identified unless other legal means hold such as the patient's consent. This is set out clearly in the *NHS* policy and good practice guidance document Confidentiality: the NHS Code of Practice, which states the need to 'effectively anonymise' patient data prior to the non-direct care usage being made of the data. Data cannot be labelled as primary or secondary use data, it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them. Anonymised data does not fall under the requirements of GDPR.

MindLife use pseudo-anonymised data. Pseudonymisation is defined within the GDPR as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual.

MindLife supply data to secondary use organisations such as commissioning PCT's, CCG's and research bodies such as universities etc. This data must have any form of person identifiable data removed before it is sent to any secondary use organisation.

8.5 Media handling

Documents and computer media containing data, system information etc should be protected. Also disposal of backup media, paper documents, voice and other recordings, test data etc should be secure. Procedures should be defined for securely handling, transporting and storing backup media and system documentation.

8.6 Exchange of information

Information exchanges between MindLife and other organisations must be controlled. Information exchanges should also comply with applicable legislation. Security procedures and standards should be in place to protect information and physical media *in transit*, including electronic messaging such as email, EDI etc and business information systems. Please refer to the MindLife Personal Data Sharing agreement.

It should not be assumed that other premises have the same level of security.

MindLife does not share personal information such as onward referrals with any third party organisation or individual that does not have the appropriate security in place. MindLife recognises that it is necessary to perform checks on those organisations to ensure there is a robust evidence of performance to the required standards.

Fax machines must only be used when absolutely necessary. If used, good practice guidelines must be adhered to.

The HSCN Network and internet are not secure for the transmission of personal or patient information without further protection such as encryption or by use of the NHS mail system. This area is subject to a wider policy from the Department of Health and the British Medical Association.

8.6.1 Email

All employees, contractors, sub-contractors and temporary staff are responsible for their personal use of email facilities provided to or used by the business.

The IT Manager is responsible for providing and maintaining a standard email disclaimer and for setting and monitoring acceptable usage and mailbox rules.

The Information Security Officer shall ensure adequate corporate anti-virus protection and cryptographic controls for email exist in line with published NHS Good Practice Guidelines.

Expected and Acceptable Uses:

The MindLife e-mail service may only be used for legitimate authorised purposes. Email may not be used for communicating illegal material, defamatory content, personal harassment, non-business purchases, or for publishing unauthorised views or opinions that may be damaging to the business.

Use of the e-mail service may be monitored for compliance with this policy.

All emails shall have an inserted footer that contains a legal disclaimer. Users of the service may not alter or delete this.

MindLife's e-mail service may only be used for the communication of information in accordance with the Information Governance policy.

The communication of confidential or restricted information by email must be appropriately protected using approved cryptographic controls (currently AES 256 bit strength or equivalent) or by using the NHS mail secure email system.

Email users must avoid opening incoming e-mail attachments that have not been checked for possible viruses or other malware in case they cause damage or disruption to the service.

8.6.2 Safe Haven Principles

A safe haven is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves MindLife whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven principles. These principles are listed as an appendix to the rear of this document - Guidance for the storage and communication of personal and sensitive data.

8.6 Mobile Computing

Extra care must be taken when using laptop, palmtop or smartphone computing devices.

When connected to the business through external telecommunication systems, a secure level of authorisation and identification must be established.

This should be in accordance with the Acceptable Use of Portable Computing Devices, Mobile Phones and Removable Media Policy – see Appendix.

All mobile devices must be password protected and if used to record person identifiable data must have this data stored in an encrypted form.

Mobile devices represent an additional risk due to their susceptibility to loss, theft or damage. All mobile equipment serial numbers must be recorded.

Care must be taken to ensure that the data entered remotely is transferred as soon as possible to MindLife systems and removed from the portable device.

Where possible additional measures for laptop protection should be employed such as the use of physical cable and locks to additionally secure the device in high risk areas.

8.7 Disposal of Information & Equipment

Information containing personal details no longer required must be disposed of in accordance with the procedure in the appendix to the rear of this document.

Computer disks and equipment that contain personal data must have that information permanently deleted or destroyed.

Note: Re-formatting a disk or a hard-drive does not guarantee that the information is permanently deleted.

8.8 Clear Desk Policy

MindLife Ltd staff and contractors must ensure that all sensitive documents and information, when not in use, are removed from desktops and computer screens and correctly filed.

This also applies in the service delivery aspect of the business where MindLife staff and contractors are working away from the office. Items such as Patient letters, consent forms etc must be protected from unauthorised access or viewing.

9 Access control

Logical access to IT systems, networks and data must be suitably controlled to prevent unauthorised use. All login names and password should be kept in a secure log file. Only authorised people have access to these records.

9.1 User access management

The allocation of access rights to users should be formally controlled through user registration and administration procedures, including special restrictions over the allocation of privileges and management of passwords and regular access rights reviews.

9.2 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls *e.g*. choosing strong passwords and keeping them confidential. Systems and information should be secured when left unattended.

9.3 Network access control

Access to network services should be controlled, both within the organisation and between organisations. Remote users (and possibly equipment) should be suitably authenticated. Patient data

must not be copied to personal computers in any circumstance. Information services, users and systems should be segregated into separate logical network domains. Network connections and routine access should be controlled where necessary.

9.4 Operating system access control

Operating system access control facilities and utilities (such as user authentication with unique user IDs and managed passwords, recording use of privileges and system security alarms) should be used. Access to powerful system utilities should be controlled and inactivity timeouts should be applied.

9.5 Application and information access control

Access to and within application systems should be controlled in accordance with a defined access control policy. Particularly applications dealing with personal special category data may require dedicated (isolated) platforms, and/or additional controls if run on shared platforms.

9.6 Mobile computing and teleworking

All portable PCs, Laptops, Mobiles etc, should be password protected; teleworking ("working from home", and other forms of mobile or remote working) should be secure. All offline devices that are used for the collection of personal or sensitive data should be encrypted.

9.7 Firewalls

Firewalls are an essential part of security of the MindLife network. Each path through the firewall should be justified and the associated service/application listed. These paths should be reviewed at least every year or additionally when significant system changes occur. Permission to establish new paths will be granted by only when there is an important business case. The default behaviour of any MindLife firewall should be to block access. Highly privileged access such as backend database administration should be restricted to access from only known IP addresses. Only senior personnel with highly privileged access accounts will be allowed to change firewall settings.

9.8 Multi-Factor Authentication

Highly privileged access should be restricted by multi-factor authentication which requires the use of a one-time code as well as a user name and password combination.

10 Information Quality and Record Management

MindLife should have in place a process for documenting its activities in respect of records management. This should take into account the legislative and regulatory environment in which the organisation operates. Records of operational activities should be complete and accurate in order to allow employees within MindLife and their successors to undertake appropriate actions in the context of their responsibilities, to protect the legal and other rights of the organisation, patients, employees and other people affected by its actions.

Records created by MindLife should be arranged in a record keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information.

10.1 Information Quality Assurance

In the context of records management, MindLife staff need to have a full understanding of:

- What they are recording and how it should be recorded;

- Why they are recording it;
- How to validate information with the patient or against other records and source material, to ensure that staff are recording correct data
- How to identify and correct errors so that staff know how to correct errors and how to report errors if they find them
- The use of information, so that staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important) and;
- How to update information and add in information from other sources.

10.2 Record Keeping

Implementing and maintaining an effective records management system depends on knowing what records are held, where they are stored, who manages them, in what format they are made accessible and their relationship to organisational functions. A records inventory will be undertaken to meet this requirement. Records keeping systems whether paper or electronic, should include a documented set of rules for referencing, titling, indexing and if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information when it is needed to maintain security and confidentiality.

10.3 Record Maintenance

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time and that there is an auditable trail of records transactions. If the record is physical such as paper based consent forms the storage accommodation should be clean and tidy, secure, should prevent damage to the records and should provide a safe working environment for staff.

For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access and readable information. Equipment to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information corresponding to its frequency of use.

10.4 Auditing

Access through viewing, creating, moving, amending or deleting records should have a secure auditable trail that details the user, time and actions of any changes made. This audit trail should be kept securely with highly restricted access applied.

10.5 Retention, Appraisal and Disposal Arrangements

When paper records are no longer required for business purposes, their placement in a designated secondary offsite storage area may be a more economical and efficient way to store them. Arrangements for offsite storage should take full account of the need to preserve important information and keep it confidential and secure.

Appraisal refers to the process of determining whether records are worthy of permanent preservation. This should be undertaken as part of the inventory process for each department.

The retention schedules outlined in the Department of Health's Records Management NHS Code of Practice will be used for all sets of records. These minimum retention periods will be identified as part of the inventory process. The appraisal process will ensure that the records are examined at the appropriate time to determine whether or not they need to be retained for a longer period than is specified in the retention schedule. This decision will be made by a senior manager who has an appropriate understanding of the operational area to which the records relate.

11 Information systems, acquisition, development and maintenance

Information security must be taken into account in the Systems Development Lifecycle (SDLC) and is part of the ISO13485 quality system processes for specifying, building/acquiring, testing, implementing and maintaining IT systems.

11.1 Security requirements of information systems

Automated and manual security control requirements should be analysed and fully identified during the requirements stage of the systems development or acquisition process, and incorporated into business cases. Purchased software should be formally tested for security, and any issues risk-assessed.

11.2 Correct processing in application systems

Data entry, processing and output validation controls and message authentication should be provided to mitigate the associated integrity risks.

11.3 Cryptographic controls

Encryption should be applied to all personal data wherever possible. All encryption products, standards and procedures used to protect personal data must be ones which have received substantial public review and have been proven to work effectively. Encryption should meet or exceed NHS standards for patient data. Cryptographic keys should be managed in such a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person. Keys must be stored and always communicated securely. When a key holder leaves the company the keys must be revoked.

11.4 Security of system files

Access to system files (both executable programs and source code) and test data should be controlled.

11.5 Security in development and support processes

Technical managers should be responsible for controlling access to project and support environments. Formal change control processes should be applied. Packaged applications should ideally not be modified. Checks should be made for information leakage for example via covert channels and trojans if these are a concern.

11.6 Technical vulnerability management

Technical vulnerabilities in systems and applications should be controlled by monitoring for the announcement of relevant security vulnerabilities, and risk-assessing and applying relevant security patches promptly. Server patches should initially be verified within a staging environment. Within 30 days of release critical security patches will be applied to all production servers. Workstations and laptops will have automatic updates enabled.

11.7 Data Protection Impact Assessment

All new project, processes and systems (including hardware and software) which are introduced must comply with confidentiality, privacy and data protection requirements. To test against the mandatory requirements MindLife will use a ‘Data Protection Impact Assessment’ (DPIA).

Each MindLife manager that is responsible for introducing new processes or procedures has the responsibility to complete and produce a DPIA, whilst all employees have a duty to promote privacy and data protection principles. Please refer to the MindLife guidance on DPIA's and contact the MindLife data protection officer.

11.8 Release Process

Releases into the production environment should be controlled. Any release into the production environment should be signed off prior to release by MindLife management. Releases should be carried out in such a way as to minimise inconvenience to system users.

12 Information security incident management

Information security events, incidents and weaknesses (including near-misses) should be promptly reported and properly managed. There must be a central point of contact, and all employees, contractors *etc*. should be informed of their incident reporting responsibilities. The term is quite broad and includes any incident that relates to loss, disclosure, denial of access, destruction or modification of MindLife's information or information assets.

Examples of security events, incidents and weaknesses are:

- Using another user's login or smart card.
- Unauthorised disclosure of information.
- Theft or loss of equipment or information.
- Inappropriate access to personal records
- Unauthorised copying of data onto portable devices.
- Malicious damage to information assets.

The above list is not definitive and is given as example only. When in doubt, report the event to the MindLife's Caldicott Guardian or Data Protection Officer.

12.1 Reporting in information security events and weaknesses

Any incident leading to a breach of security of the business or information held within it such as personal or sensitive data of patients must be reported immediately to the appropriate line manager and they will escalate the report to the MindLife Caldicott Guardian or Data Protection Officer.

All incidents must then be recorded using the MindLife Incident reporting procedure and additionally reported to the client. The incident reporting procedure requires the incident to be recorded on the online IG Toolkit Incident Reporting Tool. These incidents will either be IG SIRI's (serious incident requiring investigation) or Cyber SIRI's or a combination of both. All IG incidents level 2 or above automatically get reported to the ICO, Department of Health and NHS Digital using the tool. Near misses should also be reported as lessons learnt from this can go on to improve MindLife security.

Refer to the MindLife Incident Reporting Procedure and Guidance (Information Governance and Cyber) for a comprehensive checklist and procedure. This guide also provides a scoring mechanism for assessing the seriousness of the incident taking into account scale and sensitivity.

12.2 Management of information security incidents and improvements

Responsibilities and procedures are required to manage incidents consistently and effectively, to implement continuous improvement (learning the lessons), and to collect forensic evidence. Please

refer to the MindLife Incident Reporting Procedure and Guidance (Information Governance and Cyber).

13 Compliance

Security and compliance with this policy will be reviewed and audited on regular bases.

13.1 Compliance with legal requirements

The organisation must comply with applicable legislation such as copyright, data protection, and protection of financial data and other vital records, cryptography restrictions, rules of evidence *etc*.

13.1.1 GDPR / Data Protection Act 2018

This Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). It applies to information which relates to living individuals. The information may be processed by computer or held and stored in hard copy. Health records are specifically mentioned in the Act.

The business must discharge its responsibilities under the Act including compliance with the seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Note: GDPR requires registration with the ICO every year. Notification information can be found on the Information Commissioner's website www.dataprotection.gov.uk. It is the responsibility of the Mindlife Data Protection Officer to ensure this registration is up to date and relevant.

Mindlife's Registration Number:	ZA527795

13.1.2 Individual Rights Requests

GDPR allows certain rights to data subjects.

Summary of Individual rights

- a right of access to a copy of the information comprised in their personal data
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- a right to claim compensation for damages caused by a breach of the Act

The individual data subject has a right to apply for access to personal data of which they are subject, a right to a description of the data, the purpose of the processing and if the information is to be

shared, who it will be shared with. This must be supplied in permanent intelligible form (medical abbreviations etc explained). This information or any actions arising from the request must be carried out within one month of the request being made.

The only exceptions are if it is believed information in the records would cause serious harm to the patient's physical or mental health, or if the records or information identify or concern another person (eg, a child) who believed the information was confidential.

If an individual feels we have measured or recorded something wrongly then we can amend the patient record on request or re-measure it if it is clinically significant. If it is a difference in opinion i.e. the clinician has a clinical opinion different to that of the individual, then both positions will be held on file. In terms of clinical records, by law, this must not be altered after the event so any rectification will be recorded in a subsequent note and where possible the previous record, if written, struck through.

A personal representative or any person who may have a claim arising out of the patient's death has a right of access to the relevant part of the deceased's health record.

The Caldicott Guardian or Data Protection Officer at MindLife is responsible for dealing with individual rights requests and all MindLife staff must refer rights requests to them as quickly as reasonably practical.

Procedure for Individual Rights Request

- The individual right request is passed to the MindLife Data Protection Officer or Caldicott Guardian.
- The request is checked to see if it is a valid individual rights request.
- The request is checked to ensure all the data required is present in order to proceed.
- The ID of the requester is verified to ensure that they are the subject of the request.
- The requester is contacted to let them know the request is being processed.
- An individual rights request is opened in the Individual rights request log.
- The individual rights request is actioned
- The information requested or actions are communicated with the requester within 1 month.
- The individual rights request log is closed.

13.1.3 Freedom of Information Requests

Freedom of Information requests applies to all public bodies including government departments, the police, local authorities, schools, hospitals and surgeries. MindLife as a private organisation does not fall under the Freedom of Information Act although the GDPR and requests for access to personal data do apply.

It should be noted that under contractual arrangements with public bodies for the provision of goods and services details of these arrangements could be released when a freedom of information request is received by that public body.

13.1.4 Access to Medical Reports Act 1988

This Act gives a right of access by individuals to reports relating to themselves provided by medical practitioners for employment or insurance purposes. This Act has not been superseded by the Data Protection Act 1998 and therefore remains in force.

13.1.5 Computer Misuse Act 1990

This legislation created three criminal offences related to computer systems:

1. Unauthorised access

2. Unauthorised access with the intent to commit or facilitate the commission of further offences

3. Unauthorised modification

The Information Security officer should be notified immediately if there is a suspicion that any of these offences are, or may be, being committed.

13.1.6 Copyright, Designs and Patents Act 1988

This Act makes the use of un-licensed (pirated) software a criminal offence which could lead to fines and imprisonment.

13.2 Compliance with security policies and standards, and technical compliance

Managers and system owners must ensure compliance with security policies and standards, for example through regular platform security reviews, penetration tests *etc*. undertaken by competent testers.

13.3 Information systems audit considerations

Audits should be carefully planned to minimise disruption to operations.

14 Risk Assessment

It is important to ensure that all staff and assets are secure to prevent unauthorised access, damage and interference to the daily workings of the business.

- The business will carry out a risk assessment which assesses whether adequate measures are in place.
- If adequate measures are not in place, appropriate action will be considered to reduce the level of risk.

Effective security measures are essential for protection against a risk of an event occurring, or to reduce the impact of such an event. Such events may be accidental or a deliberate act of sabotage.

A range of security measures will be deployed to address: -

The **Threat** of something damaging the Confidentiality, Integrity or Availability of information held on systems or manual records

The **Impact** that such a threat would have if it occurred

The **Probability** of such a threat occurring

MindLife staff is encouraged to consider the risks associated with the way in which they work, the computer systems involved and the information that is held.

Appendix 1 - Confidentiality Agreement for MindLife Employees

This Agreement outlines your personal responsibility concerning security and confidentiality of information (relating to patients, staff or the business)

In the course of your employment or associated work with MindLife Ltd or after your employment or associated work ends, you may have had access to, seen or heard confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. Unless acting on the instructions of an authorised MindLife Ltd employee, on no account should such information be divulged or discussed except in the performance of your normal duties. Breach of confidence, including the improper passing of registered computer data, will result in disciplinary action which may lead to your dismissal.

You should also be aware that regardless of any action taken by the business, a breach of confidence could result in a civil action against you for damages.

You must ensure that all records, including paper copies, computer screens and computer printouts of registered data, are never left in such a manner that unauthorised persons can obtain access to them. Computer screens must always be cleared when left unattended and you must ensure that you log out of computer systems, removing your password. All computer passwords must be kept confidential.

You understand that your use of any MindLife system can be monitored and audited. This includes email, internet and app use, phone use and patient and service user systems

You must immediately report all security breaches, suspected security breaches or any other concern that might result in compromising the security and confidentiality of information (relating to patients, staff or the business) to the Caldicott Guardian or Data Protection Officer of MindLife Ltd.

No unauthorised use Mindlife IT systems or facilities is allowed.

I understand that I am bound by a duty of confidentiality and agree to adhere to the above conditions and my personal responsibilities to comply with the requirements of the General Data Protection Regulation (GDPR).

Appendix 2 - MindLife Guidance on the lawful and appropriate sharing of confidential personal information.

Gain consent where possible / appropriate

The general principle of gaining consent for the disclosure of personal information is always to be considered as a priority. There may be cases where the gaining of consent causes difficulties, or would prejudice the purposes of the disclosure in support of the protection of the individual. Where it is strongly justified, the sender may rely upon the relaxations allowed in law for disclosure without consent.

MindLife policy is to ensure that service user consent is obtained before proceeding with any data collection activity.

Keep subject fully informed

In order to comply with the GDPR, to validate implied consent if necessary and to satisfy moral obligations, the sender must always strive to fully inform the subject wherever possible of the uses to which their information will be put, what disclosures could be envisaged and what the consequences of the processing are. All parties must strive to be open and transparent.

MindLife policy is to ensure that the service user fully understands what they are consenting to by use of a comprehensive consent form either in physical or electronic form which lists how the information will be stored, what it is used for and where it will be sent. The options shown must be of the opt-in type and must not be pre-filled. No data collection activity should begin until the service users consent is given.

Keep records of disclosure

The sending party is to keep full records of disclosure of information, and to manage those records in a manner commensurate with their confidential nature.

MindLife policy is to manage consent forms in line with any other person identifiable data and the policy is outlined in this manual.

Minimise data items

The sending party must minimise the data items it discloses. Forms completed for this purpose should not have data items filled in where there is no justification for the disclosure and collection of such information. For example it will not be important in all cases for items such as ethnic group, or religious beliefs to be disclosed, where it has no bearing on the case; although it will in others. Should the recipient require fuller information, and it can be justified, the sending party will consider disclosing those items.

MindLife's policy is only to send the data necessary for the required purpose.

Select an appropriate secure transmission method

The sender is responsible for ensuring the method of transmission is the most secure available commensurate with the urgency of the case. Wherever possible, the use of Safe Haven procedures should be followed. The use of E-mail for the external transfer of the personal information covered by this policy is prohibited unless that e-mail is encrypted or securely contained within the NHSmail system.

MindLife follows the above guidance and the policy for exchange of information is defined elsewhere in this manual.

Caldicott Principles for information disclosure

1. Justify the purpose(s)
Every proposed use or transfer of person-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

2. Don't use person-identifiable information unless it is absolutely necessary
Person-identifiable information items should not be used unless there is no alternative.

3. Use the minimum necessary person-identifiable information
Where use of person-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

4. Access to person-identifiable information
Only those individuals who need access to person-identifiable information should have access to it, and they should only have access to the information items that they need to see.

5. Everyone should be aware of their responsibilities.
Action should be taken to ensure that those handling service user-identifiable information, both clinical and non-clinical staff, are aware of their responsibilities and obligations to respect confidentiality.

6. Understand and comply with the law

Every use of person-identifiable information must be lawful. The Data Protection Officer is responsible for ensuring that the organisation complies with legal requirements.

Appendix 3 - MindLife Email Policy

Email Policy Scope:

All individuals who are authorised to use MindLife Ltd's e-mail facilities are required to comply with this policy.

Individual Responsibilities:

All employees, contractors, sub-contractors and temporary staff are responsible for their personal use of email facilities provided to or used by the business.

The IT Manager is responsible for providing and maintaining a standard email disclaimer and for setting and monitoring acceptable usage and mailbox rules.

The IT Manager is responsible for identifying appropriate training materials to ensure that users of the e-mail service are aware of the provided email functionality and their responsibilities for good working practices.

The Data Protection Officer shall respond to and manage reported information security incidents, and shall ensure adequate corporate anti-virus protection and cryptographic controls exist in line with published NHS Good Practice Guidelines

Expected and Acceptable Uses:

MindLife Ltd's e-mail service may only be used for legitimate authorised purposes. Email may not be used for communicating illegal material, defamatory content, personal harassment, non- business purchases, or for publishing unauthorised views or opinions that may be damaging to the business. Use of the e-mail service may be monitored for compliance with this policy.

All emails shall have an inserted footer that contains a legal disclaimer. Users of the service may not alter or delete this.

MindLife Ltd's e-mail service may only be used for the communication of information in accordance with the Information Governance and security policy.

The communication of confidential or restricted information by email must be appropriately protected using approved cryptographic controls (currently AES 256 bit strength or equivalent).

Email users must avoid opening incoming e-mail attachments that have not been checked for possible viruses or other malware in case they cause damage or disruption to the service.

Appendix 4 - The Use of Portable Computer Devices, Mobile Phones and Removable Media

Introduction

MindLife operates and maintains cloud based servers which securely hold patient identifiable data. However it is recognised that occasionally portable media might be required to temporarily hold patient data. This guidance aims to support staff that might need to use these devices by ensuring they are aware of information and security issues.

Definitions:

Portable Computer Devices — this includes supported laptops, notebooks, tablet computers, PDA's (personal digital assistants) and mobile phones.
Removable Data Storage Media — this includes any physical item that can be used to store and/ or move information and requires another device to access it. For example, CDs, DVDs, floppy discs, tape or digital storage devices (flash memory cards, USB disc keys and portable hard drives). Essentially anything you can copy, save and/or write data to which can then be taken away and restored on another computer.
Business-supported — this includes portable computer devices and removable data storage media purchased or authorised by MindLife Ltd. It does not include any devices brought into the business from a previous organisation or anything bought without prior authorisation by the IT Department.

Scope

This guidance applies to all staff including contractors, temporary staff and volunteers.

Usage

Only authorised staff should have access to business supported portable computer devices and digital storage devices such as flash cards, USB pen drives and portable hard drives.
Storage of personal or sensitive data on removable data storage media is strongly discouraged but can be used in exceptional circumstance where no other method can be found for data transfer. In this case the storage media used should be a MindLife asset (owned and issued by MindLife) and either be a device that is encrypted by design or any files stored on the removable data storage media should be encrypted by another method before transfer onto that media. Staff using this method should be familiar with how to encrypt data and once transferred the files should be checked to ensure that encryption has been achieved successfully. Passwords for the encrypted files should be secured securely and away from the data that they encrypt.
Portable Computer Devices used for storing any personal or sensitive data should be a MindLife asset (owned and issued by MindLife) and should be whole disk encrypted using appropriate hardware/software methods.
Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action.
Staff should not use their own (or any unauthorised) portable device or digital storage device for the storage of patient personal or personal sensitive information.

MindLife Guidance on the use of portable computers:

DO ...	DO NOT...
Ensure the device being used is part of the appropriate MindLife Asset register.	Use portable computer devices outside business premises without authorisation
Store portable equipment securely when not in use – both on and off site. Use physical locking mechanisms to secure portable equipment wherever possible.	Leave portable equipment in places where a thief can easily steal them
Ensure a nominated person is responsible for each item of portable equipment.	Leave portable equipment visible in the car when traveling between locations
Ensure device / application access is password protected if the device supports it.	Leave equipment unattended in a public place
Ensure files containing personal or confidential data are adequately protected e.g. encrypted	Disable the ant-virus protection software
Ensure that where possible devices / application access once locked require password authentication to resume use.	Install unauthorised software or download software/data from the Internet
Be aware that software and any data files created by staff on MindLife portable computer devices are the property of the business	Use your own portable computer device or digital storage device such as flash cards, USB sticks and portable hard drives for business purposes unless authorised by Mindlife Management. .
Use and regularly update anti-virus software	Allow unauthorised personnel or friends or relatives to use portable equipment in your charge.
Where portable equipment is pooled, maintain a register to enable identification of current user	Delay in reporting lost or stolen equipment
Obtain authorisation prior to the removal of portable equipment from the premises	Attach unauthorised equipment to the network
Report immediately any stolen equipment to the police and line manager	Remove person identifiable information off site without authorisation from your Manager
Ensure that when portable devices are disposed of/re-issued MindLife disposal / re-issue procedures are followed.	
Ensure that portable devices are returned to the business if you are leaving employment.	

Appendix 5 - Disposal and Re-issue of Computer Devices and Media

When an item requires disposal or is no longer required then the following procedures should be followed:

Computers

Great care should be taken when disposing of either desktop or laptop computers. If they are to be sold to another person, the hard disk should be securely wiped using appropriate specialised software in order to render any data irrecoverable. Computers which are to be scrapped should have the hard disk destroyed.

Floppy Disks/CD-Rom/Tapes

These items should be re-used/destroyed locally. If the items contain personal or confidential information this must be removed before re-issue or if requiring disposal they should be shredded or incinerated.

USB sticks, PDAs etc:

These items can be re-issued within the business but the asset register must be updated accordingly and any personal/confidential information removed. If the item is no longer required then it should be disposed of correctly and the appropriate Asset Register noted accordingly.

Appendix 6 - Third Party Supplier Agreement

This agreement is for third party suppliers requiring access to MindLife's Clinical Systems. By completing and signing this formal request for access, the supplier certifies that he understands that:

- Information concerning patients or staff is strictly confidential and must not be disclosed to unauthorised persons. This obligation shall continue in perpetuity.
- Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the Data Protection Act 2018 or an action for civil damages under the same Act in addition to any disciplinary action taken by the business.

Further, the Supplier certifies that:

- They will not give access to any of MindLife's networks to any external organisation unless that body has been formally authorised by the business to have such access.
- The Information Commissioner has been appropriately notified that it will be processing personal data.
- It is legally entitled to undertake the work agreed in the contract agreed with the business.
- It will abide by the requirements set out in MindLife's Supplier Code of Practice below for handling any of the personal data/information disclosed to their organisation during the performance of such contracts

Access on the above terms is requested by:

Please complete in clear BLOCK CAPITALS

Company Name:	
Company Representative's Name:	
Proposed purpose for access:	
Approximate Duration:	
Signature and Date	
Approved By:	
Signature and Date:	

MindLife Supplier Code of Practice (Page 1 of 2)

This Code of Practice applies where access is obtained to any personal data/information (as defined in the Data Protection Act 2018) held by the business for the purpose of development, preventative maintenance, fault diagnosis, hardware or software testing, repair, upgrade, replacement or any other related activity.

The access referred to in paragraph 1 above may include:

- Access to data/information on MindLife cloud based servers
- Access to data/information on MindLife premises
- Access to data/information from a remote site
- Examination, testing and repair of media (e.g. disc drives)
- Examination of software data dumps.
- Processing using MindLife's Ltd data/information

The Supplier must certify that his organisation has notified the Information Commissioner that he is processing personal data (Data Protection Act 2018) and that he is legally entitled to undertake the work proposed.

The Supplier must undertake not to transfer the personal data/information out of the EEA unless such a transfer has been registered, approved by the business and the country to which information is to be transferred has been deemed to have an adequate level of protection for personal information, or is a USA company which has signed up to abide by the US-EU privacy shield principles.

The work shall be done solely by authorised employees, servants or agents of the supplier who are aware of their personal responsibilities under the Data Protection Act 2018 to maintain the security of the personal data/information held by Mindlife.

While the data/information is in the custody of the Supplier it shall be kept in appropriately secure means.

Any data/information sent from one place to another by or for the Supplier shall be carried out be secure means. These places should be within the Supplier's own organisation or an approved sub-contractor.

Data/Information which can identify any patient/employee of the business must only be transferred electronically if previously agreed by the business. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 1998 and ISO 27002. This will also apply to any direct-dial access to a computer held database by the Supplier or their agent.

The data/information must not be copied for another purpose than that agreed by the Supplier and MindLife Ltd.

Where personal data/information is recorded in any intelligible form, it shall either be returned to the business on completion of the work or disposed of by agreed secure means and a certificate of secure disposal shall be issued.

MindLife Supplier Code of Practice (Page 2 of 2)

Where the Supplier intends to sub-contracts any work for the purposes in paragraph 1 above, Mindlife will be required to authorise this before any work commences and shall require the sub-contractor to observe the same standards as outlined in this code of conduct.

The business shall, wherever practical, arrange for the equipment or software to be maintained, repaired or tested using anonymised data that does not include the disclosure of any personal data/information. The business reserves the right to audit the Supplier's contractual responsibilities or to have those audits carried out by a third party.

The business will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the Supplier's employees and/or any agents and/or sub-contractors.

Any security breaches made by the Supplier's employees, agents or sub-contractors will immediately be reported to the Data Protection Officer of the business.

Appendix 7 – Guidance for the storage and communication of personal and sensitive data

The following outlines guidance on the use of various communication methods used within MindLife,

Transmission of Personal Information via Email

It is MindLife policy that all personal and personal sensitive data is protected before it is emailed. This must be achieved by means of encryption using a suitable method. Word and Excel provide inbuilt methods for encrypting documents. PDF documents containing personal or sensitive data can also be encrypted with appropriate software. Please refer to other documentation or ask a colleague how to do this if you are unsure. Ensure that the password to unlock the information is sent by other means or has been pre-arranged by the recipient. If you are still unsure please contact MindLife's Data Protection Officer. It is a serious disciplinary offence to not follow the correct procedure. The body of the email should contain no personal or sensitive data.

The NHSmail system is automatically encrypted for communication. If (and only if) you are using the MindLife NHS mail account you do not need to additionally encrypt attached documents as long as the email you are sending is being sent to another nhs.net account.

The following rules apply:

- Create the document or spreadsheet that contains the personal or sensitive information.
- Encrypt the file
- Attach it to the email – check the recipient is correct
- Re-check the attachment by opening it from the pending email
- Check the data in the email is correct and there is no other data that should not be there
- Check the recipient is correct again
- Communicate the password to the recipient by another means – SMS text, phone call,etc
- Send the email
- Check the email has been received by the intended recipient
- Ensure that any locally stored unencrypted files created during this process are deleted from your PC.

Fax machines

Fax machines must only be used to transfer personal information where it is absolutely necessary.

The following rules must apply:

- Ensure it is sited in an area that is restricted to those who need to access the information.
- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct.
- Notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- Care is taken in dialling the correct number.
- Confidential faxes are not left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent.
- All confidential faxes sent should be clearly marked" Private and Confidential" on the front sheet

.

Post

- Outgoing mail should be sealed securely and marked "private and confidential" if it contains person-identifiable information.
- Risk assess and use registered post if appropriate

Paper Documents

- All personal records must be stored face down in public areas and not left unsupervised.
- Information that is no longer required (e.g. post it notes, messages) should be shredded or disposed of using shredders of appropriate security rating.
- When no longer being actively used or overnight personal records should be locked away in lockable filing cabinets

Computers

- Do not share log-ons and passwords with anyone.
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data.
- PCs or laptops should be locked or switched off when you are away from your desk for any length of time.
- Wherever possible laptops should be physically secured if being used in public locations.
- Laptops and where possible desktop PCs should be whole disk encrypted using appropriate software/hardware protection.
- MIndlife patient Information must not be saved or copied into any PC or media that is not a registered MindLife asset
- All person-identifiable information sent by email must be sent from one NHSmail address to another secure e mail domain such as NHS.net to NHS.net or via an encrypted attachment over normal email.

Telephone Calls

- Do not make telephone calls of a confidential nature involving patients where you can be overheard by anyone not bound by the MindLife confidentiality requirements.
- When you receive a call check to ensure you are speaking to the correct person, ring back (where possible) to confirm someone's identity.
- Personal Information must not be left on an answer machine or mobile messaging service. It is permissible to leave a message saying the recipient should contact MindLife but the message must not contain any other details including details of what the call is about. If the call is returned ensure you are speaking to the correct person.

Communications by Text Message

Although it may be desirable to communicate with individuals in this way, there are potential information security risks that should be considered before you do so. For example:

- Are you confident that the person using the recipient mobile is the person to whom the message is intended?
- Can you be sure that you are using the correct phone number?
- Can you be sure that the patient has received the message?
- Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) – as mobile phones are easy to misplace or may get stolen there is a danger of a breach of confidentiality occurring that the patient may find embarrassing or damaging.
- Mobile phone networks may be open to additional risks of eavesdropping or interception. If you decide to go ahead with this method of communication, you should ensure you send the minimum amount of confidential data possible.

Physical Location and Security

- Do not allow unauthorised people into areas where confidential information is kept unless supervised.
- Store person-identifiable information in a locked draw/filing cabinet.

Information Governance and Security Policy Communication Record

I confirm that I have read and understood the MindLife Information Governance and Security Policy Manual and confidentiality agreement and undertake to comply with its requirements:

This includes

The MindLife Information Governance and Security Policy Manual.

And the appendices

The Confidentiality Agreement for MindLife Employees and Contractors

MindLife Guidance on the lawful and appropriate sharing of confidential personal information and Caldicott principles.

The MindLife Email Policy

Guidance on the use of portable computer devices, mobile phones and removable media

Guidance on the disposal and re-issue of computer devices and media

Guidance for the communication of personal and sensitive data

NAME OF ORGANISATION:	**MindLife Ltd**
FULL NAME: (In Clear BLOCK CAPITALS)	
POSITION:	
SIGNATURE:	
DATE:	

PLEASE ENSURE THIS IS SIGNED, DATED AND RETURNED TO bridget.ramsey@mindlife.net EITHER IN PAPER FORM OR BY SCANNING ELECTRONICALLYe