Information Systems Acceptable Use Policy

Inmind Reference:	GDPR06
Category:	GDPR Policies
Version Number:	1.4
Reviewed on:	January 2019
Next review date:	February 2020
Lead Officer:	Contracts Director
Equality Impact Assessment completed:	Yes

Applicable Legislation/Regulations:
The Data Protection Act 1998 The Care Act 2014
Codes of Practice:
Purpose:
To ensure the proper use of Inmind Healthcare Group's electronic information systems. To set out what Inmind deems the acceptable and unacceptable use of these systems and Inmind's policy regarding such use.

Version Control Table		
Date Ratified	**Version Number**	**Status**
February 2018	1.3	Closed
January 2019	1.4	Live

Date	**Key Revision**
16/02/18	Format change only
24/01/19	Changed Lead Officer

Please check to ensure this is the most current electronic copy of this document as it is updated and published in electronic format only (hard copies may become out of date).

1.0 The Policy

a) Information is an asset, like any other business asset it has a value and must be protected

b) The systems that enable us to store, process and communicate this information must also be protected

c) 'Information Systems' is the collective term for our information and the systems we use to store, process and communicate our information

d) The practice of protecting our information systems is known as 'Information Security'

e) Inmind has implemented an 'Information Governance Framework in order to manage and continually improve Information Security over time

f) This policy covers three specific areas:

- Use of information systems within the Inmind environment
- Use of mobile devices both within and outside the Inmind environment
- Actions to be taken in case of an actual or potential information security breach

g) This policy is introduced to staff at the time of their induction and updated on a regular basis.

h) The primary purpose of the policy is to minimise the potential risks of harm to Inmind, its Service Users and its employees through misuse of information systems.

i) It is intended to ensure that Inmind complies with relevant current legislation and other standards which govern this area of business by providing a set of policies, guidelines and instructions on the use of IT Systems by Inmind Employees.

j) Failure to comply with this policy can lead to disciplinary action as detailed in Inmind's Disciplinary Procedures.

2.0 The Procedure

2.1 General

a) In general, all employees are authorised to use the internet and external e-mail as a means of communication for the purposes of Inmind business.

b) Registered Managers shall maintain a central up-to-date list of the location of all computers in their Units and grant specific authorisation if these computers are to be removed from those locations.

c) The IT Department, together with Registered Managers shall ensure that a system for maintenance of Inmind computers is in operation at all Units and that arrangements are in place for employees to report, without delay, to a designated person(s) any faults, loss, or damage to computer equipment.

d) Registered Managers shall issue a list for their Unit setting out the following details:
- the designated person(s) to whom any faults are to be reported;
- tracker to indicate employees have read and understood this AUP

e) In the event of a member of staff leaving Inmind, head office is to inform the IT Department of the individual's details in order to disable the computer account.

f) Inmind regards the IT Systems (which in this policy means the computers and all supporting equipment and software applications) in its Units as a vital and integral part of its business.

g) Inmind expects all its employees to use computers reasonably and for the purposes only of Inmind business. All users of Inmind computer systems must note that the Computer Misuse Act 1990 makes it a criminal offence for an unauthorised person to illegally access, attempt such access or misuse a computer.

h) Inmind will take seriously any actual, attempted or suspected infringement of this policy, and may take disciplinary action against any employee acting or attempting to act in breach of this policy, which may result in dismissal in serious cases.

i) Employees shall not: -

- Make changes to the hardware or software content or configuration of, nor delete any software from any computer owned by Inmind without the prior consent of the Registered Manager and/or IT Department
- Attempt to circumvent any of the legitimate controls in place to govern the acceptable use of information systems
- Use personal computer equipment (including smart phones, PDAs, netbooks ?? and similar devices) within Inmind premises without specific permission from the Registered Manager.

- Use Inmind computers, or seek information held on them unless this is directly relevant to and necessary for the performance of their jobs.
- Introduce onto or use on any Inmind computer any removable media containing non-work-related material. Removable media which contain work related material form part of the intellectual property of Inmind and employees shall exercise care and caution when using, storing, transporting them, whether within or outside Inmind's premises.
- Move any Inmind computers from their original location without the prior knowledge and consent of the Registered Manager.

2.2 Monitoring

a) All employees shall be aware that: Inmind reserves the right to monitor:

- And access any or all areas of any computer and software systems which it owns, including e-mail boxes and messages
- All internet access and act against any illegal activity and / or non-Inmind business related activity

b) No employee shall be entitled to assume that any information held on a computer owned by Inmind is private and confidential to him/her.

c) Inmind may electronically audit its computers on a regular basis to ensure that all software used is legally installed and licensed.

2.3 Security

a) **General**

- Employees must not disclose to any non-Inmind personnel or company any information about Inmind's IT systems, which may make them vulnerable to any third party.
- Employees shall only use those screen savers supplied with the operating system. No other screensavers are to be installed.

b) **Physical**

Employees shall:

- Be responsible for the safety and maintenance of computer equipment supplied by Inmind and the proper use and security of software and data stored either on that equipment or other equipment which they can access remotely
- Protect computer equipment from potential physical damage by direct sunlight, spilled liquids and similar dangers

c) **Passwords**

Computer system passwords provided to members of staff are changed by the IT department following specific request and authorisation. Users will not be allowed to use the same password as that which has expired nor will blank passwords be allowed.

Passwords must:

- Not be names or have other obvious connection to the user
- Be changed regularly and not be repeated
- Be a mixture of letters, numbers and symbols
- Be a minimum of 7 characters in length
- Be kept secret
- Not be shared or disclosed to ANY party, even if they claim to be from the IT Department, management or an external party such as the police.

Employees shall:

- Keep their personal passwords confidential and are advised to use passwords which are free from personal data (such as birthdates, etc.)
- Ensure that if their password security be compromised then the password is to be changed immediately and the matter brought to the attention of the IT Helpdesk

Employees shall not allow people who are not authorised users to have access to Inmind information systems or use an employee's personal login

d) **Sensitive Data/Confidentiality**

Employees shall not transmit by computer confidential information about or relating to the business of Inmind, its Service Users, clients, suppliers or contacts, unless done so in the course of the bona-fide performance of their job. Confidential information shall not be left on display on an unattended computer.

All processing of personal data must be undertaken only in accordance with the requirements of Inmind's Confidentiality Policy.

Such processing must only be carried out on computers owned by Inmind which are connected to the corporate network or on lap tops as provided by Inmind and for which specific permission of their use has been granted.

'Processing' means obtaining, recording or holding information or data or carrying out any operation or set of operations on information or data, including: -

- Organising, adapting or altering it
- Retrieving, consulting or using it
- Disclosing it by transmission, dissemination or otherwise making it available

- Aligning, combining, blocking, erasing or destroying it.

'Personal data' is any information relating to any individual who can be identified from that information.

2.4 Software

a) Employees are warned that it is illegal to make copies of software used on Inmind computers. Software issued by Inmind is licensed to Inmind and is protected by copyright law.

b) Inmind may audit its computers on a regular basis to ascertain whether all the software loaded onto its systems is legal. The audit is checked and reconciled with the software licence library and all unauthorised software is deleted. The source of the unauthorised software will be ascertained, and disciplinary action may be taken against the employee who installed it.

c) Computer software is solely to be installed by the IT Helpdesk or authorised personnel. As a result:

- Any software received by e-mail is not to be opened, run or installed. This includes files but not limited to; *.exe, *.bat, *.scr, *.vbs, *.eml. Receipts of such files are to be notified to the IT Helpdesk.

- No 'freeware' or ‘Shareware’ or other software of any kind shall be downloaded from the Internet or otherwise installed by employees on any Inmind computer unless specifically authorised, in writing, by the Registered Manager or the IT Department.

- Games shall not be permitted on Inmind computers except for those provided with the operating system, installed by the IT Department, or for educational purposes, after being specifically authorised, in writing, by the Registered Manager or a member of senior management delegated to act on such matters.

- Downloading of trial software or software updates for hardware and software is to be carried out only where such downloading has first been approved or instructed to do so, in writing, by the IT Department. Once any such trial software has exceeded its unlicensed lifetime, the software is to be uninstalled or the correct license purchased

- Any software legally and with proper prior authority downloaded via the internet is to be checked with anti-virus software prior to installation on an Inmind computer.

2.5 Email

a) External e-mail facilities are provided for all staff and is only for use in connection with the proper performance of the users' duties for Inmind.

b) Employees shall not: -

- Allow E-mail facilities to be used by non-authorised personnel or transfer or confer e-mail privileges to other individuals.
- Use e-mail systems and accounts for which they are not authorised
- Send personal e-mail
- Transmit confidential information about or relating to the business of Inmind, its Service Users, clients, suppliers or contacts unless done so in the bona fide performance of their job.
- Transmit any information by text, picture, sound or programme which is or may be libellous, obscene, illegal, sexually explicit, political, bullying, campaign orientated, discriminatory or disparaging of others. This will not be condoned or tolerated. Non-compliance with this policy may result in disciplinary action.
- Transmit commercial software or any copyrighted materials belonging to third parties or Inmind.
- Transmit chain and other fund-raising letters.
- Use private mobile or other devices to synchronise or download corporate e-mails without specific authorisation by head office.

c) Employees shall be aware of the following guidelines relating to the use of e-mail: -

- E-mail is a non-secure medium and care shall be taken when composing, sending and storing messages. It is possible that messages will not be received at their destination and that they can be intercepted. If e-mail is used for critical business communications confirmation of receipt by another means must be ascertained.
- Outgoing e-mails shall be regarded in the same way as any other business correspondence and shall be treated as a company record.
- Employees shall be reminded that material via e-mail, which they find acceptable, might be offensive to others, e.g. jokes. Care shall be taken in what is sent by e-mail and its use shall not become a substitute for 'one to one' conversations.
- Offers and contracts made by e-mail are considered as legally binding.
- As e-mail is immediate and cannot be withdrawn once 'sent', care shall be taken when constructing e-mails.
- E-mails can be used as evidence in a court of law.
- Complaints and criticism shall not be dealt with by e-mail.
- Outgoing e-mails have a default footer with an associated disclaimer. This must not be modified without prior authorisation from the IT Department.

2.6 Internet

a) Inmind is committed to providing Internet access where necessary for business related purposes.

b) Restricted internet access is provided to authorised employees for work related purposes only. As such, employees shall not: -

- Visit any pornographic website or any other website, the visiting or use of which could bring Inmind into disrepute;
- Visit any other sites not related to and/or necessary for the proper performance by the employee of his/her duties for Inmind;
- Use Instant Messaging for private use
- Use the internet for freelance business, access to "chat rooms", gambling, illegal or political activity or any activity which is not related to and/or necessary for the proper performance by an employee of his/her duties for Inmind and/or which is contrary to the interests of Inmind.
- Use the Inmind internet facility for private use.
- Use the internet as a communication medium where any unauthorised commitment is made on behalf of the organisation or where commitments are received (e.g. from suppliers).
- Download from the Internet any material that is deemed or may be deemed indecent, offensive, malicious, or of an inflammatory nature.

2.7 Viruses

a) All employees shall: -

- Be vigilant in trying to prevent viruses being introduced into the Inmind network. Any employee wilfully or negligently introducing a virus into the network may be subject to disciplinary action.
- Inform the IT Helpdesk immediately in the event of a virus being identified/ suspected as being present upon an Inmind computer or being identified as being present upon transportable media.

b) Employees shall not carry out ANY remedial work notified by e-mail of virus activity nor are they to forward such alerts. Receipts of such e-mails are to be reported personally or by telephone to the IT Helpdesk.

2.8 Laptops

a) All aspects of policy specified in the previous sections apply to laptops, together with the additional policy items contained in this section.

b) Each device will be registered to a named and specific user who will be accountable for it.
It is noted that laptop users may have a need to carry out non-business-related internet

viewing and the sending of personal e-mails whilst away on legitimate Inmind business. In this instance both personal e-mail and internet use are allowed provided that the other related provisions of this policy are adhered to.

c) Employees shall: -

- Protect their laptop from physical hazards, including spilling liquids, food substances, hot car interiors etc, always.
- Store and carry their laptop in the Inmind–supplied case to reduce the risk of accidental damage.
- Routinely connect their laptop to the internet to ensure that the anti-virus software can be updated.
- Wherever possible, store data on Inmind's file servers, as the hard drive of a laptop computer is not a secure storage medium

d) Employees shall not: -

- Loan their laptop to work colleagues, relatives, friends or any other person. Laptops are specifically provided for the use of the individual to whom issued
- Leave their laptops unattended.
- Advertise the presence of their laptop in a public place.
- Leave their laptop in an unattended vehicle.
- Display sensitive information in a public place (e.g. a train) where the screen could be overlooked.
- As a rule, store personal or commercially sensitive information on their laptop. Where this is necessary, the data shall be stored in a password- protected, 256-bit encrypted files.

2.9 Reporting Information Security Incidents

a) If any employee becomes aware of any actual or possible breach of information security, it is their duty to report this to the IT Department as soon as possible. Furthermore, if any employee becomes aware of a situation which could give rise to such an incident, it is equally important to report this.

b) On discovering a breach, an employee shall take all reasonable steps to prevent any further breach. For example, if a virus were detected on a system, then the system shall be removed from any network to which it is attached and closed consistent with the recommendations of the software reporting the problem to the line manager/IT department.

c) Once the immediate problem has been addressed, an Incident Log Report is to be completed. This will include details of the discoverer, and the time and date of discovery. It also required classification of the Incident as indicated in the table below.

d) The incident should also be described, with reference to any error messages, warnings or other notifications which may have been received.

e) On completion, the incident log shall be signed, dated and given to the staff member's line manager who will forward a copy to the SIRO You may want to change this to the Director of Governance or whoever is going to be responsible for maintaining the Information Risk Log.

f) On resolution, details of the actions taken will be relayed back to the local line manager together with any recommendations or changes to operating methods which may be considered relevant.

Category	Options	Comments
Type of incident	Confidentiality Integrity Availability	Relates to Service User or commercial data Relates to quality or reliability of data Relates to ability to process data
Impact on Department	Total failure Service impairment No effect	Department or staff prevented from working Temporary service impairment, catch up possible No significant impact on operations
System affected	Service User information Finance Email Internet Etc.	Specifies the system which was affected.

Appendix 1

Equality Impact Assessment for this policy

Protected Characteristic (domain)	Area of conflict	Resolution
Age	Nil	N/A
Disability	Nil	N/A
Gender Reassignment	Nil	N/A
Pregnancy & Maternity	Nil	N/A
Race	Nil	N/A
Religion or Belief	Nil	N/A
Sex	Nil	N/A
Sexual Orientation	Nil	N/A
Marriage and Civil Partnership	Nil	N/A

All relevant persons are required to comply with this policy and must demonstrate sensitivity and competence in relation to diversity in race, faith, age, gender, disability and sexual orientation. If you feel you are disadvantaged by this policy, please contact the Registered Manager and the service will actively respond to the enquiry.