Magpas AIR AMBULANCE

POLICY

Data Security and Protection

Position responsible: Data Protection Officer
Approved by: ELT

Issue Date : July 2021
Review Date : April 2023

Related Documents	Leaving Policy Significant Event Reporting Policy Risk Management Policy Information Governance Manual Corporate Data Retention Policy Clinical Records Management Clinical Governance Policy
Further information	Data Protection Act 2018 Copyright, Designs and Patents Act 1988 Computer Misuse Act 1990 EU Directive on Protection of Individuals 1995 General Data Protection Regulation Barclays Policy for Credit Card Security Committed Giving Policy

1.0 Background

1.1.1 This policy is required due to the increasing reliance on information management and technology (IM&T) in supporting the delivery of health care, fundraising, finance and Human Resource Management makes it necessary to ensure computer systems are developed, used and maintained in a secure manner to protect data. The General Data Protection Regulation requires organisations to have a Data Protection Officer (DPO). The DPO for Magpas is the Chief Executive Officer.

1.2 The purpose of this Policy is to protect Magpas from data protection security risks and to ensure the data held in its information systems is secure from unauthorised modification, disclosure, or loss, whether accidental, deliberate, internal, or external. It is intended to ensure the confidentiality, integrity and availability of data, as defined below:

- Confidentiality - data access is confined to those with specified authority to view
- Integrity - all system assets are operated correctly and according to specification
- Availability - information is accessible to the right person at the right time

1.3 Scope

1.3.1 This policy applies to all Magpas employees and volunteers, and the IM&T facilities located and used on its sites, whether provided "in-house" or through third party managed service support contracts. It imposes the same duties and responsibilities on all other organisations and their employees that may use Magpas facilities, and also third-party support organisations and their employees or volunteers.

1.3.2 Magpas Air Ambulance may use third party organisations to carry out electronic services related to banking and the processing of donations. In the event that third parties are used Magpas will ensure that the third party has the appropriate security and data protection measures in place and these are obtained in writing and reviewed regularly. Magpas adheres to all policies relating to banking procedures.

1.4 Magpas will comply with all legislation relating to Data Protection and IM&T security. The most significant being:

- Data Protection Act (2018)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- EU Directive on Protection of Individuals (1995)
- General Data Protection Regulation (2018)

There also exists a common law obligation to preserve the confidentiality of personal data.

1.5 Format and standards

1.5.1 The detail of this policy (as set out in the following sections) follows the structure, requirements, recommendations and guidance provided by the NHS Records Management Code of Practice for Health and Social Care 2016 (published by the Information Governance Alliance).

1.5.2 The policy aims to ensure:

- Data storage systems are properly assessed for security.
- Appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and systems.
- All staff are made aware of the limits of their authority and their accountability.
- A means is established to communicate appropriate guidance on IM&T security issues.

This Policy is the highest level of data protection security guidance in Magpas.

1.6 Implementation and Compliance

1.6.1 A risk assessment will be carried out if the following circumstances occur:

- New system installation.
- Major system modifications.
- Increase of security risks/exposure.
- Increase of overall system security level.
- Serious security violations (defined by the adverse incident matrix).
- Security evaluations and/or audits.

1.7 Review

1.7.1 This Policy will be reviewed annually or more frequently if required by changes in legislation, standards, or practises. New security control strategies from the risk assessment are incorporated in the policy.

2.0 Policy Management

Objective of section: To manage information security within Magpas.

2.1 The Magpas Research Governance Framework and the Magpas Clinical Governance structure refer to this policy.

2.2 Overall responsibility for maintaining and implementing this policy lies with the Executive Leadership Team (ELT). The Executive Leadership Team will be responsible for identifying assets (equipment, systems and data sets) and for assigning an “owner” for each (designations for any level of corporate responsibility are the responsibility of the Trustee Board as per the Magpas Constitution).

2.3 All staff will be responsible for ensuring the protection of data assets within their area and also for ensuring compliance with this policy and the performance of specific security processes or procedures that relate to the data assets for which they have responsibility.

2.4 Magpas will ensure the policy is made available to all staff, by bringing its existence to the attention of all staff and publishing it in the means most appropriate to gain widest exposure. This will be done in the form of updates that are disseminated in a format that is accessible and understandable.

3.0 Information Dissemination

Objective of section: To ensure all staff are aware of data protection security threats and concerns, and are equipped to support the policy in the course of their normal work thereby reducing the risks of human error, theft, fraud or misuse of data storage facilities.

3.1 Security will be addressed at recruitment stage and included in job descriptions and contracts, and will be monitored during employment. Reference requests during recruitment should also refer to data security.

3.2 Job descriptions will define security roles and responsibilities as laid down in this policy.

3.3 Magpas will ensure that where a member of staff is required to use IM&T facilities to fulfil their job role, they are briefed on this policy and associated legislation. Staff will also be made aware they are personally accountable for the functions they perform, and disciplinary procedures may be invoked should they be responsible for a breach of security.

3.4 Where practical, there will be segregation of functions and separation of duties, so tasks having an IM&T security element are not performed by the same person; thereby minimising threats to security.

3.5 A job function that could allow fraud or theft should be part of the responsibility of more than one person

3.6 For critical systems and tasks, expertise should be invested in more than one member of staff, so in the event of absence, work may be continued. Dependence on key individuals should also be reduced by the use of procedures documentation.

3.7 Each member of staff must be made aware of the extent of their authority, from individual tasks to budgetary responsibility.

3.8 IM&T security privileges and access rights will be allocated on the basis of specific job function and not on status.

3.9 Staff must declare personal interest in circumstances that could lead to a conflict of interest; e.g. where a relative or friend has been treated by the service or where IM&T procurement decisions could be influenced.

3.10.1 Where these staff are not already covered by a non-disclosure undertaking in their contract, they should be required to sign such a confidentiality agreement committing them to the same codes of conduct and discipline as permanent staff, before they are provided with access to Magpas IM&T facilities.

3.10.2 Where agency staff are employed, these conditions should form a part of the contract of engagement with the agency. If work of a more sensitive nature is carried out by contract or agency staff, extra conditions may be identified and imposed in accordance with this greater risk.

3.11 Users of IM&T facilities should sign a non-disclosure undertaking (confidentiality agreement). This should form part of the contract of employment with the member of staff or any volunteer, with the conditions clearly explained.

3.12 Confidentiality agreements will be the subject of review where there are changes to terms and conditions of volunteers, employed staff or other contractors' employment.

3.13 When an employee leaves the organisation:

- The relevant line manager should confirm the confidentiality agreement continues to apply, even though the person is leaving.
- System passwords must be disabled, thereby denying further access.
- All relevant departments should be informed of the changes and the volunteer's or employee's name removed from the Magpas lists.
- All relevant staff should be informed of the termination, to ensure the individual is treated as a visitor.
- Employees working a notice period should, if considered necessary, be assigned to non-sensitive tasks, or otherwise appropriately monitored.

3.14 Magpas property should be returned; particularly personal identification devices, entry keys and other access items.

3.16 Particular attention should be paid to the above requirements if the termination is not 'amicable'. The relationship between the employee and the charity should be assessed so the extent of the implementation of 'leaving measures' can be carried out at an appropriate level. e.g. – an employee leaving on good relations may retain all privileges until the day of leaving.

4.0 Responsibility for Control of Assets

Objective of section: To ensure the responsibility for the security of all IM&T assets is assigned.

4.1 All major data assets will be accounted for and have an assigned 'owner', responsible for maintaining appropriate security measures. Responsibility for implementing security measures may be delegated, but accountability will remain with the assigned owner of the asset.

4.2 Information security classifications will be used to indicate the level and priority of system and data security protection, as follows:

- Special Category Data (class 1): where data held is of a highly sensitive nature and where security will be at the highest level – e.g. data relating to specific identifiable (named) patients patient report forms (PRF) and coroner or police statements, donors' bank details, staff medical records or mental health reports.
- Personal Data (class 2): where data is not of the most sensitive nature but still requires strict security – e.g. all patient data other than those in class 1, along with the personal data of individual staff.
- Ordinary (class 3): where data is not patient based or personally identifiable but nevertheless security is required. Data in this class will normally be aggregated or lists – e.g. mailing lists, such as staff, volunteers, donors or contacts lists.

4.3 All information that requires a Class 1 (extremely sensitive) classification must be identified and the appropriate manager responsible must take appropriate steps to ensure its security and confidentiality.

- The designated owner of Class 1 information held regarding patients is the Medical Director.

4.4 Each line manager is responsible for the security, integrity and confidentiality of the Magpas administrative paper and electronic information and has the following responsibilities.

- Identifying all the data within their area of responsibility (completed most recently in the staff survey).
- Specifying/agreeing how the data can be used, who can use the data and what type of access each user is allowed.
- Determining and reviewing the classification (Class 1, 2 or 3) of the data.
- Approving appropriate security protection.
- Ensuring compliance with security controls and legislation covering personal or medical data.
- Ensuring compliance with data protection act.

4.5 Reviews should be carried out periodically to confirm appropriateness of classification; e.g. where data has been made public it ceases to be sensitive.

4.6 The Caldicott Report on confidentiality of patient information recommended that a senior health professional in each NHS organisation be nominated as the Caldicott Guardian (of personally identifiable patient information). Although Magpas is not an NHS organisation, the links to the NHS are so strong that compliance with the Caldicott Report is considered essential. The Caldicott Guardian for Magpas is Alistair Steel, Deputy Medical Director.

4.7 The Medical Director is the identifiable head of clinical information assets. The charity's Chief Executive Officer (CEO) is the IM&T asset owner for all Media and PR.

4.8 It is the responsibility of each director, as the major IM&T asset owner, to ensure each directorate complies with data protection policy, that compliance is audited, and systems improvement opportunities are implemented.

4.9 The Senior Information Risk Officer (SIRO) will ensure implementation of all data IM&T security systems improvement opportunities from audit, activity and recommendations are implemented and audited. The SIRO for Magpas is the Director of Operations.

5.0 Access Control to Secure Areas

Objective of section: To describe the physical measures within Magpas to prevent unauthorised access, damage and interference to IM&T services.

5.1 IM&T facilities supporting critical or sensitive activities will be housed in secure areas and protected from unauthorised access, with security based on defined perimeters and achieved through physical barriers - i.e. critical installations will be protected at least by lock and key.

5.2 The information is secured within indexed locked cabinets, the keys to which are not allowed off site and are stored within a key safe in the Executive Assistant's office.

5.3 All system processors file servers and network equipment will be located in lockable cabinets or in secure areas secured to the building, with access controlled through secure doors.

5.4 Unauthorised visitors will not be allowed in designated secure IM&T areas and authorised visitors will not be left unaccompanied. Staff will be instructed to challenge anyone unknown to them in designated secure areas.

5.5 All staff will be issued with an identification badge, which must be worn at all times.

5.6 External organisations whose systems or other IT infrastructure are housed in Magpas IM&T locations will only have access to their own systems.

5.7 Authorised visitors will sign a confidentiality agreement and are entered into a visitor's log.

6.0 Equipment Protection and Security.

Objective of section: Power supply protection, IM&T support and IM&T asset acquisition.

6.1 Protection of IM&T equipment is necessary to reduce the risk of unauthorised access to data and to safeguard against equipment loss or damage. IM&T equipment will be physically protected from security risks and environmental hazards.

6.2 An appropriate environment, including temperature monitoring, uninterrupted power supply (UPS) and fire protection, is available and used for critical IM&T equipment.

6.3 Critical equipment will be protected from power failure. A suitable power supply, as recommended by manufacturers' specifications, is available for the main server, supported by back-up generator power where deemed appropriate. Critical IM&T equipment will also be protected by UPS (uninterruptible power supply) equipment.

6.4 All cabling installed within buildings will be installed within the framework of the building, or within surface-mounted conduit, and be to appropriate standards. Exposed cabling is secured to the building and contained within a suitable cable tidy device.

6.5 Ongoing maintenance of IM&T equipment will normally be the subject of a maintenance contract. All central file server and network equipment is covered by maintenance contracts.

6.6 IM&T equipment will only be taken off-site with the appropriate manager approval. Portable computers should be protected by suitable access protection and staff with authorisation to take equipment off-site should ensure it is given a high level of protection – i.e. equipment must not be left in cars, etc., as this represents a significant risk to the equipment and data.

6.7 Purchase, installation, relocation and disposal of IM&T assets will be according to relevant Magpas policies and procedures. Purchases of IT equipment must only be made in accordance with Magpas polices, and be agreed within each directorate's financial framework. The acquisition of new IM&T assets must be presented by the directorate asset owner to the CEO and Honorary Treasurer

6.8 An up-to-date register of acquisitions and disposals of IM&T assets will be maintained by the Senior Information Risk Officer (SIRO). This will include the location, serial number, purchase price, technical description and system manager, or user primarily responsible for the asset.

6.9 Donated assets must be notified to the appropriate manager, who will approve, oversee installation and record the equipment.

7.0 Computer and Network Operations

Objective of section: To ensure the correct and secure operation of computer and network facilities.

7.1 Responsibilities and procedures for the management and operation of all computers and networks will be established and supported by appropriate training, operating instructions and documentation.

7.2 The Magpas data network will be designed and maintained to establish a secure networking infrastructure that will support secure data transfer required by Magpas and fits into the secure infrastructure programme of the wider NHS.

7.3 The CEO will be responsible for recording all proposed changes to the Magpas data network (including firewall rules table) obtaining authorisation from the Executive Leadership Team, prior to implementation.

7.4 Magpas will comply with the NHS-wide Networking Security Policy by ensuring that NHS information:

- Is not disclosed to unauthorised personnel.
- Is used only for the purpose for which it is intended.
- Has not been modified, either accidentally or maliciously.
- Is presented in the correct sequence for messaging applications.
- Is available when required.

7.5 The Code of Connection is a set of rules laid down by the NHS Information Authority (NHSIA), which must be complied with in order to connect with the NHS-wide networking infrastructure. These have been applied to Magpas. The rules refer to precautions that must be taken to protect the network and all its users:

- Access to Magpas-wide networking is protected by at least one authentication control (i.e. a password that fulfils the stipulations of this policy).
- The CEO is responsible for the security of the Magpas local area network (LAN).
- The CEO is responsible the security of the Magpas LAN to the Internet.
- All relevant staff are made aware of their responsibilities in relation to the security of the NHS-wide networking infrastructure.
- Physical access to all Magpas workstations is controlled.
- All incidents that constitute a threat to Magpas, its employees, volunteers or its partner data stakeholders are reported to the appropriate manager and graded for likelihood of reoccurrence system impact and therefore risk level.
- Advertising or other form of promotional activity for non Magpas purposes is forbidden.
- Where direct (on-line) access to NHS or Ambulance Trust systems is allowed, staff are made aware of the additional care required.
- All program/data files obtained through connection to external services are checked by an up-to-date virus checking facility before being used on any system connected to the NHS-wide networking infrastructure.
- Where Magpas provides a permanent host system on the Internet or any related service, there shall be no connection between the host system and NHS-wide network services.
- All changes to the Magpas firewall rule table will be submitted to the CEO for approval prior to implementation of those changes.

8.0 Security Incident Management

Objective of section: To ensure IM&T security incidents are detected, reported, investigated and managed appropriately.

8.1 This section is based heavily on the Magpas Incident Reporting and Risk Assessment Policy.

8.2 The CEO will establish and maintain a formal procedure for reporting security incidents.

8.3 It is the responsibility of each staff member to document a potential near-miss or actual security incident on the Magpas Significant Event Report Form

8.4 Once reported the incident will be scaled for severity.

8.5 The severity of the incident defines the time frame in which action must be taken and which of staff must be involved.

8.6 An IM&T security incident is defined as having resulted in:

- The unauthorised disclosure of confidential information.
- The integrity of a system or data being put at risk.

- The availability of a system or data being put at risk.
- An adverse impact - e.g.
  - Embarrassment to Magpas.
  - Threat to personal safety or privacy.
  - Legal obligation or penalty.
  - Financial loss.
  - Disruption of activities.

8.7 Usual incident - such an event is one that is considered to be an everyday event – e.g. entering an incorrect password or ID by mistake, or forgetting to change a password within the required time period. There are likely to be a number of such events and it should be the aim to collect statistics on these events automatically from systems.

8.8 Unusual incident - these events range from minor to major – e.g. something unexpected happening to a data file, or to a breach of security where a person (whether a member of staff, or not) acts suspiciously in relation to a computer system.

8.9 Unusual incidents, or information indicating a suspected or actual security breach, must be reported to the appropriate manager at the earliest opportunity, for investigation.

9.0 System Planning, Procurement and Acceptance

Objective of section: To ensure appropriate security requirements are included in systems procurements.

9.1 All security requirements should be identified at the system requirements phase of a project and included in the procurement business case.

9.2 Implementing any necessary security requirements should be built into the project implementation plan. The plan should be ratified by the CEO.

9.3 Procurement procedures should ensure:

- Any hardware or software changes that may affect network management are taken into account.
- Mandatory and desirable security requirements are included in procurement specifications.
- The CEO is consulted to ensure the selected system will meet security requirements.

9.4 Procurement procedures should also consider the implications on disaster recovery plans in terms of compatibility with the existing plans.

9.5 Contracts should not be awarded until security requirements are satisfied and financial implications are approved by the CEO and Executive Leadership Team.

10.0 Protection from Malicious Software

Objective of section: To safeguard the integrity of software and data.

10.1 Precautions will be taken to prevent and detect the introduction of malicious software and all staff will be alerted to the risks of malicious software.

10.2 The IT support company will, where possible, ensure measures are in place to prevent or detect the introduction of viruses on PCs.

10.3 Only authorised and appropriately licensed and approved software will be permitted on Magpas PCs and servers. The use of unlicensed software is prohibited and line managers are authorised to remove such software from Magpas equipment.

10.4 Procedures will be established to minimise the risk of the introduction of viruses:

- Staff and volunteers will be briefed on the dangers of malicious software.
- Staff and volunteers will be responsible for ensuring all computer media they bring in to or take out of, Magpas, and all data or software they import or export via a network, is virus checked.
- Appropriate backup procedures will be established to facilitate the restoration of virus infected systems.
- PCs and servers will be regularly checked for viruses, with virus checking software being regularly updated. Where possible, antivirus software updates will be installed on PCs automatically over the data network.
- CD drives will be disabled in PCs installed in potentially ‘vulnerable’ areas to reduce the risk of virus infection.

10.5 Procedures will be established for checking and disinfecting any device suspected of holding malicious software:

- Any PC or server suspected of being infected by a virus must be immediately isolated and reported to the line manager.
- Use of the infected machine will be prohibited until agreed by the line manager.
- All software and data on the machine will be checked for the presence of viruses and virus checking of all other possibly infected machines will be carried out.
- A security incident report will be completed by the Magpas ~~Incident Reporting System~~ significant event reporting system.

11.0 Information Redundancy and Back-Up

Objective of section: To maintain the integrity and availability of IM&T services and to prevent damage to IM&T assets.

11.1 Magpas data will be protected by clearly defined and controlled back-up procedures that generate data for archiving and contingency recovery purposes. Archived and recovery data will be accorded the same security as live data.

11.2 Procedures will be established for backing-up data, logging events and faults, and, where appropriate, monitoring IM&T equipment environment. Operating procedures documentation will include protection of media, data and systems from damage, theft and unauthorised access.

11.3 The Executive Assistant (EA) to the CEO will be responsible for backing-up all central systems, with daily backup regimes documented in the relevant system operational procedures.

11.4 There should be provision for periodic off-site contingency testing of central system backup DVDs, where their viability can be proved.

11.5 Staff and volunteers within departmental systems will be responsible for undertaking and documenting back-up procedures for their systems. Backup plans should be agreed with the CEO and, where practical, include provision for off-site secure fireproof storage and regular restoration testing.

11.6 All sensitive and confidential data (and non-sensitive data where the quantity of data makes back-up from a PC impractical) should be held on servers located in central IM&T facilities.

11.7 Redundant backup media will be securely disposed of. The EA to the CEO will be responsible for the secure disposal of backup media for centrally managed systems.

12.0 Data and Software Exchange

Objective of section: To prevent loss, modification or misuse of data during transfer or exchange.

12.1 Reliable couriers will be used at all times for the transport of data media. Where necessary special measures will be adopted to protect sensitive information from unauthorised disclosure (e.g. locked containers).

12.2 When using e-mail, staff should be particularly aware of:

- Vulnerability to unauthorised interception or modification.
- Vulnerability to incorrect addressing.
- Publication of directory entries.
- Remote access to the e-mail system and accounts.
- The need to exclude sensitive information from the system.
- The exclusion of inappropriate third parties from e-mail.

12.3 Users of e-mail and internet facilities will be required to be trained and sign acceptance of policies covering these facilities before being granted access to them.

12.4 Subject to the availability of resources, e-mail and internet access will be monitored to ensure proper use.

13.0 User Access Control

Objective of section: To restrict access to Magpas information to authorised users.

13.1 Access to computer services and to data will be controlled on the basis of Magpas requirements, and will take account of policies for information dissemination and entitlement, for example the ISP.

13.2 There will be formal procedures to control access rights to IM&T services and systems, with special attention being given to the control of allocation of privileged access rights that allow users to override system controls or access Security Level 1 information.

13.3 Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

13.4 Magpas will aim to comply with the NHS Net Full Code of Connection requirements, as identified in Section 7 (Magpas Networks & NHS network Operations) of this policy.

13.5 The operational requirements for access control will be defined and documented for each system. The documentation will clearly define the access rights of each user or group of users.

13.6 There will be a formal documented user registration and de-registration procedure for access to all IM&T services and systems, that will:

- Confirm the user has authorisation from the appropriate manager.
- Confirm the level is appropriate for the purpose.
- Ensure access is not granted until the authorisation process is complete.
- Maintain a register of staff and volunteers authorised to use each system.
- Assess access rights of users who change responsibilities and where appropriate amend access levels.

- Remove access rights of users leaving Magpas.
- Periodically review users' access rights.

13.7 The special privileges allocated to a system manager or administrator give access to routines that expose the vulnerabilities of a system. The allocation of special privileges for network and other central systems will be controlled and an authorisation process will be established which:

- Identifies who should have special privileges.
- Can allocate and revoke special privileges on an ad hoc basis.
- Maintain a record of who has been allocated special privileges.

13.8 Users will be briefed on the importance of passwords and advised as to their appropriate use:

- Passwords must not be displayed on screens as they are entered.
- When allocated a new or temporary password for start-up use by the systems manager or administrator, the user must immediately change it.
- Password changes must require authentication by re-entering.
- A Password must have the following qualities:
    - Minimum eight characters,
    - Consisting of four numbers and four letters
    - The letters must not be producing any readily identifiable word.
    - The numbers selected must not have personal relevance.
- Passwords must be disabled on change of staff, or staff resignation.
- System users must have their own passwords. Sharing of passwords or the use of generic passwords is not permissible.
- Passwords must not be written down.
- Password must be changed regularly, and changed immediately where some form of compromise is suspected.

13.9 Network and system intrusion detection will be deployed where resources allow and all suspected violations or attempted violations will be reported as a security incident

14.0 Computer Access Control

Objective of section: To prevent unauthorised computer access.

14.1 Access to computer facilities will be restricted to authorised users. Computer systems that serve multiple users should be capable of the following:

- Identifying and verifying the identity and the location of each user.
- Recording successful and unsuccessful system accesses.
- Controlling the connection times of users.

14.2 Access to IM&T services will be via secure log-on procedures designed to minimise the opportunity for unauthorised access. The log-on process should:

- Not display system or application identifiers.
- Display a notice stating the system should only be used by authorised users.
- Not provide log-on help.
- Validate log-on information after all data input.
- Limit unsuccessful attempts to access the system to three.
- On failure to log-on due to too many attempts, register the attempt, force a time delay to the next series of attempts and disconnect the data link.

- Limit the time allowed to access. Failure due to time should be regarded as a failure equivalent to failing after more than three attempts.
- Display information about the last successful log-on to allow checking by the authorised user.

14.3 Each user should have a unique identifier, which gives no indication of the privilege level.

14.4 Inactive terminals will time-out to a screen saver after a specified period of time. All screen savers should be password protected.

14.5 Users should ensure PCs and terminals are logged off when left unattended.

14.6 Remote access to systems will comply with NHSIA Security guidelines. System suppliers that require on-line access to investigate or fix faults will be permitted access.

14.7 Any supplier requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives.

15.0 Application Access Control

Objective of section: To prevent unauthorised access to data held in IM&T systems.

15.1 Logical access controls should restrict access to application systems and data to authorised users.

15.2 Applications should:

- Control user access to data and application system functions.
- Provide protection from unauthorised access to software capable of overriding application controls.

15.3 Access to data will only be granted to staff who require it to perform their job function.

15.4 Special arrangements will be available for emergency purposes (e.g. access to support maintenance staff or engineers), where the password should be changed at the completion of the emergency activity.

15.5 All detected unauthorised attempts at access should be reported as a security incident

15.6 The use of systems utilities will be controlled and restricted. Control should be of the following type:

- Password protection for system utilities.
- Segregation of system utilities from applications.
- Restriction of use to ‘trusted’ and authorised users.
- Logging of the users of the systems utilities and the levels of authorisation.

15.7 Inactive terminals will time-out to a screen saver after a specified period of time. All screen savers should be password protected.

15.8 Users will be responsible for ensuring that PCs/terminals are logged off when left unattended.

15.9 Strict control of program source libraries will be maintained, as follows:

- Program sources should not be held on operational systems.
- Programs under development should not be held on operational systems.
- Controls over access to program sources should be in place.
- Version management should be in operation to control the distribution of software.
- An audit log of access to program libraries should be maintained.

16.0 Data Validation

Objective of section: To prevent loss, modification or misuse of data.

16.1 Appropriate data validation controls, including audit trails, will be designed into application systems.

16.2 Controls will be designed into systems to ensure that:

- The integrity of data is maintained through the use of reference file data, cross checking and validation.
- Numbers of records and values etc. can be checked through systems.

16.3 Rejected data should be output, showing reason for rejection and returned to users for correction and completion.

16.4 System managers should maintain a log of any notified losses or corruption in data.

16.5 Authentication techniques should be adopted where critical or confidential data is involved.

17.0 Business Continuity Planning

Objective of section: To enable IT facilities to be restored and Magpas activities maintained after any unforeseen failure or disaster. To provide, where possible, fall-back arrangements during a period between system failure or disaster and resumption of normal service.

17.1 Business continuity plans for the restoration of critical Magpas IM&T processes and services in the event of serious interruptions will be developed and maintained. Measures will include limiting the consequences of any threats that are realised and to provide a timely resumption of essential operations.

17.2 Business continuity planning will be the responsibility of the Executive Leadership Team. The planning process will include:

- A formal documented assessment of how critical each system is, including the implications of its loss.
- A formal documented assessment of how long services could continue without each system.
- Identification and agreement of all responsibilities and emergency arrangements.
- Documentation of agreed procedures and processes.
- A formal assessment of the resilience of the plans and how quickly continuity will be achieved.

17.3 Multiple copies of plans should be kept, both on-site and off-site (e.g. at the homes of key personnel)

17.4 A business continuity planning framework will be established with the following components:

- Emergency procedures describing the actions to be taken following an incident which will jeopardise business operations.
- Fall back procedures for both short term and long term loss that describe the actions to be taken to move essential business activities to alternative locations.
- Resumption procedures that describe the actions to be taken to return to normal full operations at the original site (e.g. defined and controlled data back-up procedures).

18.0 Implementation and Compliance

Objective of section: To comply with all statutory obligations.

18.1 All relevant statutory and contractual requirements will be explicitly defined and documented. The controls, countermeasures and individual responsibilities to meet these requirements will be similarly defined and documented.

18.2 Where necessary, advice on specific legal requirements will be sought from Magpas' advisors.

18.3 No copyright material will be copied without the copyright owner's consent.

18.4 Guidelines on the retention, storage, handling and disposal of medical and other records and information will be maintained. These guidelines will aim to protect essential records and information from loss, destruction and falsification.

18.5 Magpas will designate an appropriately trained person to ensure procedures are in place to meet the requirements of the Data Protection Act (2018).

18.6 Each system owner will be responsible for ensuring the system is compliant with the Magpas Data Protection Act (2018) notification.

18.7 Magpas staff, volunteers and any third party users will be informed that no access to systems is permitted unless formal authorisation has been given. Failure to comply with this requirement could result in breach of the Computer Misuse Act (1990), which identifies the following criminal offences:

- Unauthorised access.
- Unauthorised access with intent to commit a further serious offence.
- Unauthorised modification of computer material.

19.0 Website Security, Confidentiality and Cookies

19.1 Details of how Magpas manages website security, confidentiality and cookies are included in appendix 1 – Data Security Notice.

Appendix 1 – Data Security Notice

1.0 Introduction

1.1 This data security notice is for visitors to our websites, apps and other digital platforms. It also sets out how we use cookies.

1.2 Information you give us.

1.2.1 You may give us information about you by filling in forms on our site www.magpas.co.uk (**our site**) or by corresponding with us by phone, e-mail or otherwise. This includes information you provide when you register to use our site, subscribe to participate in our lottery or raffles, sign up to volunteer, make a charitable donation, participate in social media functions on our site, enter a competition or survey, and when you report a problem with our site. The information you give us may include your name, address, e-mail address and phone number, financial and credit card information, personal description and photograph.

1.3 Information we collect about you.

1.3.1 With regard to each of your visits to our site we may automatically collect the following information:

- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;

- information about your visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our site (including date and time); products or services you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.

1.4 Information we receive from other sources.

1.4.1 We may receive information about you if you use any of the other websites we operate or the other services we provide. We are also working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies) and may receive information about you from them.

1.5 Website Cookies

1.5.1 Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. By continuing to browse the site, you are agreeing to our use of cookies.

1.5.2 A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive.

1.5.3 We use the following cookies:

- Strictly necessary cookies

These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to make use of e-billing services.

- Analytical/performance cookies
  They allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily.

- Functionality cookies
  These are used to recognise you when you return to our website.

- Targeting cookies
  These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website and the advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose.

1.5.4 Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies, over which we have no control. These cookies are likely to be analytical/performance cookies or targeting cookies.

1.5.5 You block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

2.0 Uses made of the information

2.1 We use information held about you in the following ways:

2.1.1 Information you give to us. We will use this information:

- to carry out our obligations arising from any contracts entered into between you and us and to provide you with the information, products and services that you request from us;
- to provide you with information about other goods and services we offer that are similar to those that you have already purchased or enquired about;
- to notify you about changes to our service;
- to ensure that content from our site is presented in the most effective manner for you and for your computer;
- for internal record keeping. We keep records of event participation, organisation records, volunteer records, charitable donations records, lottery membership records, financial subscription payments and records, electronic financial receipts and, information mailing, goods and services provided, donation trend and profile analysis;
- to contact you for fundraising purposes or to inform you of events or other activities or news from time to time.

2.1.2 Information we collect about you. We will use this information:

- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to improve our site to ensure that content is presented in the most effective manner for you and for your computer;
- to allow you to participate in interactive features of our service, when you choose to do so;
- as part of our efforts to keep our site safe and secure;

- to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you;
- to make suggestions and recommendations to you and other users of our site about goods or services that may interest you or them.

2.1.3 Information we receive from other sources:

- We may combine this information with information you give to us and information we collect about you. We may use this information and the combined information for the purposes set out above (depending on the types of information we receive).

2.2 Disclosure of your information

2.2.1 We may share your information with selected third parties including:

- Business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or you.

- Advertisers and advertising networks that require the data to select and serve relevant adverts to you and others. We do not disclose information about identifiable individuals to our advertisers, but we may provide them with aggregate information about our users (for example, we may inform them that 500 men aged under 30 have clicked on their advertisement on any given day). We may also use such aggregate information to help advertisers reach the kind of audience they want to target. We may make use of the personal data we have collected from you to enable us to comply with our advertisers' wishes by displaying their advertisement to that target audience.

- Analytics and search engine providers that assist us in the improvement and optimisation of our site.

2.2.2 We may disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.

- If we or substantially all of our assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.

- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation or to protect the rights, property, or safety of Magpas, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection.

2.3 Where we store your personal data

2.3.1 The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

2.3.2 All information you provide to us is stored on our secure servers. Any payment transactions will be encrypted.

2.3.3 Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

3.0 Your rights

3.1 Opting out, you have the right to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also exercise the right at any time by contacting us at info@magpas.org.uk.

3.2 Opting out, the national data opt-out applies to the disclosure of confidential patient information for purposes beyond individual care across the health and adult social care system in England. Magpas Air Ambulance will only share patient information with those NHS services necessary for providing individual care.

3.3 Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to our websites.

4.0 Access to information

4.1 The Act gives you the right to access information held about you. Your right of access can be exercised in accordance with the Act. Any access request may be subject to a fee of £10 to meet our costs in providing you with details of the information we hold about you.

5.0 Changes to our privacy policy

5.1 Any changes we may make to our privacy policy in the future will be posted on our website and where appropriate, notified to supporters by e-mail.

6.0 Contact

6.1 Questions, comments and requests regarding this policy are welcomed and should be addressed to the Data Protection Officer info@magpas.org.uk.