GENERAL PRACTICE SOLUTIONS
EXPERTLY NAVIGATING SUCCESS

71-75 Shelton Street, London, WC2H 9JQ | www.generalpracticesolutions.net
020 8865 1942 | enquiries@generalpracticesolutions.net

INFORMATION GOVERNANCE POLICIES

(COMBINED)

IRU. October 2021

PURPOSE

This policy defines General Practice Solutions (GPSs) approach to Information Governance. It provides assurance that our oganisation complies with legislation and requirements, and that information risks are appropriately recognised and managed.

The aims of this policy are:

To ensure that information (including information about identifiable people and other confidential information) are:

- Held securely.
- Obtained fairly and lawfully.
- Recorded and managed accurately and reliably.
- Used effectively and ethically.
- Shared and disclosed appropriately and lawfully.
- To ensure that information risks are identified and managed.
- To ensure that all GPS workers meet their own responsibilities and accountabilities in relation to the processing of information.
- To maximise the value of GPSs organisational information assets, through their effective and lawful management.

POLICY STATEMENT

Information is vital to GPS's role as a consultancy service to primary care client providers. Only by the effective obtaining, use and sharing of information can GPS meet its purpose to ensure that providers are safe, effective, compassionate, high-quality care and to encourage services to improve.

Failure to adequately protect and manage information would create an unacceptable risk to the privacy of people who use those services and to the privacy of other people whose information GPS may obtain and use. Failure to identify and meet our obligation of confidentiality may also create significant risks to the effectiveness of GPS's consultancy, the rights, and legitimate interests of client providers, and public trust in GPS as a consultancy agency.

GPS will maintain an 'Information Governance framework' to provide a structured and effective set of controls and measures for the handling of information.

This framework will include:

- A suite of policies covering key areas of Information Governance
- A structure of established accountabilities and responsibilities
- Guidance, processes, and training for our workers and for others who access or process information on behalf of GPS.

IRD: October 2022

SCOPE

Information governance is the process by which an organisation obtains and provides assurance that it is complying with its legal, policy and moral responsibilities in relation to the processing of information.

GPS considers that the following areas fall under the scope of information governance:

- Data protection.
- Information Security.
- Information access (including Freedom of Information).
- Knowledge and Information Management (including record management and data quality).
- Confidentiality.

All workers and agents of GPS are required to comply with this policy, and with the policies and processes that sit under it as part of the information governance framework.

RESPONSIBILITIES

The following overarching responsibilities apply to all parts of the Information Governance Policy. Additional responsibilities are listed under the relevant parts of this policy.

ROLE	RESPONSIBILITY
All staff (including those in roles below)	Processing information, managing records, and complying with security standards and requirements in line with this policy, as well as other related policies and guidance to comply with legislative and business requirements.
Directors and Customer Relation Managers (CRMs)	Ensuring that systems are in place to support compliance with information law, access and management of records, information security and continuity of service.

Executive Team (ET)	Approving and signing off relevant
Senior Information Risk Owner (SIRO)	Ownership of the Information Governance Policy. Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of GPS are identified, processed, transmitted, stored and used in line with the
The Caldicott Guardian	Providing advice and oversight to ensure that confidential personal information relating to people who use the services we regulate is obtained, used, handled, and shared in accordance with the Calidcott
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: Inform and advise on compliance with GDPR. Monitor compliance with GDPR. Cooperate with the ICO. Act as a contact point with the ICO on issues relating to processing.
Information Governance Group (IGG)	Provide the Executive Team, on policies, systems, guidance, methodologies, and training for information governance. Producing and signing off guidance and training materials on information governance issues. Maintaining and overseeing the GPS risk register.

LRD: October 2022

ASSOCIATED POLICIES

GPS will establish and maintain the following policies under our information Governance framework:

- Data protection policy.
- Information security policy.
- Freedom of Information policy.
- Knowledge and information management (KIM) policy.
- Code of Practice on Confidential Personal Informa

DATA PROTECTION POLICY

PURPOSE
This policy defines General Practice Solutions (GPSs) approach to Information Governance. It provides assurance that our clients comply with legislation and GPS's requirements, and that information risks are appropriately recognised and managed.

The aims of this policy are:

- To ensure that information (including information about identifiable people and other confidential information) are:
  - Held securely.
  - Obtained fairly and lawfully.
  - Recorded and managed accurately and reliably.
  - Used effectively and ethically.
  - Shared and disclosed appropriately and lawfully.

- To ensure that information risks are identified and managed.
- To ensure that all workers meet their own responsibilities and accountabilities in relation to the processing of information.
- To maximise the value of GPSs organisational information assets, through their effective and lawful management.

POLICY STATEMENT
Information is vital to GPS's role as a consultancy to primary care services.

Only by the effective obtaining, use and sharing of information can GPS meet its purpose to ensure that providers are safe, effective, compassionate, high-quality care and to encourage services to improve and become fully compliant with national guidance / regulations.

Failure to adequately protect and manage information would create an unacceptable risk to the privacy of people who use those services and to the privacy of other people whose information GPS may obtain and use. Failure to identify and meet our obligation of confidentiality may also create significant risks to the effectiveness of GPS's consultancy, the rights, and legitimate interests of providers of services, and public trust in GPS as a consultancy agency.

GPS will maintain an 'Information Governance framework' to provide a structured and effective set of controls and measures for the handling of information.

DEFINITIONS

Personal data is any information processed which identifies and relates to a living person. This includes information which directly identifies a living person, but also to information which is not directly identifiable, but which could be linked back to the person by reference to other information, which is held by GPS or is likely to come into the possession of GPS.

LRD. October 2021

Special category personal data is personal data which reveals or relates to physical or mental health (including health and care needs, treatment, or the use of care services), racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, sex life or sexual orientation. It also includes the processing of genetic data or biometric data (e.g. fingerprints, DNA samples, iris scans).

Processing means any operation, action on, or interaction with personal data, whether carried out by a person or by automated means.

Processing includes, but is not limited to access to, obtaining, recording, organisation or structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, sharing, publication, restriction, erasure or destruction of personal data.

Data protection law is any legislation (including Act, regulation or statutory instrument) currently in force which directly applies to the processing of personal data by any organisation.

The principle legislation at the time of publication of this policy are the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Data subjects are the people to whom personal data relates.

Privacy notices are information that is communicated to data subjects to inform them of how and for what purpose(s) their personal data will be processed by GPS, and which provide them with further information prescribed under data protection law, including information of the security and retention of the data, and on the data subject's rights.

DRD: October 2022

DATA PROTECTION PRINCIPLES

In accordance with data protection law, GPS will ensure that all processing of personal data is carried out in accordance with the principles relating to the processing of personal data (under Article 5 of GDPR).

These '**Data Protection Principles'** require that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits the identification of data subjects for no longer than is necessary.
6. Kept secure, with appropriate measures to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage.

GPS will maintain appropriate records to demonstrate compliance with the data protection principles.

LAWFUL BASES FOR PROCESSING
GPS will only process personal data or special category personal data, where we have identified that a lawful basis for doing so is engaged under data protection law. We will maintain records of the lawful bases relied upon for the processing of personal data.

CONSENT
Consent is one lawful basis for processing personal data. Explicit consent is one lawful basis for processing special category personal data.

For consent to be valid, it must be informed and freely given. Consent must be indicated by a positive action, and cannot be implied from failure to respond, object positive action, and cannot be implied from failure to respond, object positive action, and cannot be implied from failure to respond, object opt out. Consent may be withdrawn at any time and GPS must ensure that withdrawing consent is as easy as giving consent.

GPS will not rely upon consent as the *only* lawful basis for processing for the purpose of exercising our consultancy functions.

Where GPS does rely upon consent as a lawful basis for processing, we will maintain records as evidence of consent.

OTHER REQUIREMENTS OF DATA PROTECTION LAW
GPC will also comply with the other requirements of data protection law, which include (but are not limited to):

Providing privacy notices to inform data subjects as to how and why we may process their personal data, and as to their rights.

GPS will produce and publish 'privacy notices' which we shall make available on our website and, where appropriate, in other GPS publications.

Where we collect personal data directly from data subjects (e.g. on forms, webforms or surveys, or when asking for information in person or via electronic communications) we will provide a privacy notice at the point of collection.

Where we collect personal data via a third party, we will ensure that a privacy notice is communicated to the data subject to the extent that it is proportionate and reasonable in the circumstances to do so.

COMPLYING WITH THE RIGHTS OF DATA SUBJECTS.
GPS will ensure that there are processes in place to comply with the rights of data subjects. These include:

Right of data access: GPS will have a process to manage and respond to requests from data subjects for access to their own personal data and for information as to how and for what purpose(s) it is being processed by GPS.

DRAFT October 2022

Right to data portability: Where processing is based upon the lawful basis of consent, or for the performance of a contract with the data subject, GPS's process for responding to requests from data subject for access to their own personal data will allow for the data subject to receive the relevant data in a structured and machine-readable format.

Right to erasure (right to be forgotten), right to restriction of processing, and right to object to processing:
GPS will have a process to manage and respond to requests from data subjects that we should erase their personal data. GPS will have a process to manage and respond to requests from data subjects for the restriction or processing of personal data concerning him or her in specified ways or in specific circumstances. GPS will also have a process to manage and respond where a data subject objects to the processing of their personal data by GPS, on grounds relating to his or her personal situation.

These processes will recognise that these rights are qualified and may be refused where GPS needs to continue processing the personal data for legitimate reasons (with a lawful basis), including where it is necessary and in the public interest to do so for the exercise of our functions for clients.

Right to rectification: GPS will have a process to manage and respond to requests from data subjects for the rectification of inaccurate personal data concerning him or her.

Rights in relation to automated decision making, including profiling: GPS will not use automated processing, without meaningful human input, to profile individuals or make decisions which significantly affect those data subjects, other than with the explicit consent of the data subject or where the processing is explicitly laid down in law. If GPS proposes to undertake such automated processing, this will be clearly communicated in published privacy notices.

DATA PROTECTION BY DESIGN AND DEFAULT, AND DATA PROTECTION IMPACT ASSESSMENT (DPIA).
GPS will ensure that any new process or change which is likely to result in a high risk to privacy, or to the rights and freedoms of data subjects, is first subject to a DPIA.

This DPIA will include steps to establish the lawful basis for processing, and to understand and mitigate the likely risks.

The DPIA shall also ensure that the processing of personal data is minimised, and that appropriate technical and organisational measures are integral to the design and operation of systems and processes that involve processing of personal data.

ONLY TRANSFERRING PERSONAL DATA OUTSIDE OF THE UK OR EUROPEAN ECONOMIC AREA (EEA) WHERE WE HAVE ADEQUATE ASSURANCE THAT IT IS LAWFUL TO DO SO AND THAT APPROPRIATE PROTECTIONS ARE IN PLACE.
Where possible and practicable, GPS will process personal data within the UK/EEA. GPS will only process personal data outside of the UK/EEA where we have undertaken a DPIA and are satisfied that the personal data is afforded equivalent levels of protection as it would if processed within the UK/EEA, and that the transfer is lawful.

EDD: October 2022

NOTIFICATION OF DATA BREACHES.
GPS will have a process under our Information Security Policy to ensure that data protection breaches are reported to the Information Commissioner's Office, and notified to data subjects, as required under data protection law.

APPOINTING A DATA PROTECTION OFFICER (DPO) AND PROVIDING ADEQUATE RESOURCE FOR THE DPO TO PERFORM HIS ROLE.
GPS will appoint and maintain a DPO and will provide the DPO with the resources required to effectively fulfil its purpose.

LRD October 2022

CALDICOTT PRINCIPLES
The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out Principles that organisations should follow to ensure that personal data relating to people who use services is protected and only used when it is appropriate to do so.

The Principles were extended to adult social care records in 2000 and further revised in 2013. GPS will comply with the Caldicott Principles when processing personal data relating to people who use our client provider services. The Principles are:

Principle 1 - justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential personal data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - don't use personal confidential data unless it is absolutely necessary.
Confidential personal data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for people who use care services to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - use the minimum necessary personal confidential data
Where use of confidential personal data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of confidential personal data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to confidential personal data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling confidential personal data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect service-user confidentiality.

Principle 6 - comply with the law

Every use of confidential personal data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - the duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies. GPS will have a Caldicott Guardian who will advise on, and monitor compliance with, the Caldicott Principles within GPS.

LRD.October2022

CONFIDENTIAL PERSONAL INFORMATION (CPI)
Personal data that has been obtained by GPS on terms or in circumstances requiring it to be held in confidence is 'confidential personal data' (CPI) as defined by section 76 of the Health and Social Care Act 2008.

It is a criminal offence for any person to disclose CPI within the lifetime of the data subject, other than where a 'defence' to permit disclosure is met under section 77 of the same Act. GPS is required to publish a Code of Practice on Confidential Personal Information ('The Code'), setting out the practice we will follow when obtaining, handling, using and disclosing CPI.

GPS will publish the Code and keep it under review to ensure that it is, and remains, compliant with data protection law and this policy. The Code will be the principle guide for GPS workers and agents in making any decisions about the processing of CPI.

RESPONSIBILITIES
The following overarching responsibilities apply to all parts of the Data Protection Policy. Additional responsibilities are listed under the relevant parts of this policy.

ROLE	RESPONSIBILITY
All workers (including those in roles below)	Processing personal data in accordance with this policy - as well as other related policies, processes and guidance - to comply with data protection law and to appropriately protect the privacy, rights and freedoms of data subjects.
The Chief Executive Officer (CEO) and the Board of Directors	Ensuring that systems are in place to support compliance with data protection law. Ensuring that GPS has an appropriate DPO, Caldicott

	Guardian and SIRO in post, and to ensure that they have adequate resources, freedom and authority to perform those roles.
Executive Team (ET)	Approving and signing off relevant policies and processes. Ensuring that policies, processes and systems established or adopted by GPS are compliant with data protection law.
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: Inform and advise on compliance with GDPR. Monitor compliance with GDPR. Provide advice as regards data protection impact assessments. Cooperate with the ICO. Act as contact point with the ICO on issues relating to processing. To carry out these tasks with due regard to risks relating to the processing of personal data.
Senior Information Risk Owner (SIRO)	Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of GPS are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with GPS's legal, statutory and organisational requirements.' (GPS, Corporate Governance Framework) See also Scheme of Delegation
The Caldicott Guardian	Providing advice and oversight to ensure that personal data relating to people who use the services we regulate is processed in accordance with the Caldicott Principles.

LRD: October 2022

Information Governance Group (IGG)	Providing advice to the GPS Executive team, via the SIRO, on policies, systems, guidance, methodologies and training on data protection. Producing and signing off guidance and training materials on data protection issues. Maintaining and overseeing GPS's information risk register.
Information Rights Manager	Producing advice and promoting good practice across the organisation in relation to processing personal data in accordance with data protection law. Developing policies, guidance, and training. Advising and supporting on the completion and sign-off of DPIAs. Managing and overseeing the work of the Information Access Team.
Information Access Team.	Recording, coordinating and responding to subject access requests.

LRD: October 2022

MONITORING COMPLIANCE

The Information Rights Manager will provide reports on compliance with data protection law and with this policy, when appropriate, using measures agreed with the ET and IGG. These reports will be presented to the DPO, Caldicott Guardian and SIRO at IGG meetings and key issues of compliance and performance will be reported to the ET.

The DPO may report to the ET or the Board on any aspect of compliance with GDPR. In accordance with Article 38(3) of GDPR, the DPO will not be instructed or restricted in the performance of their tasks.

ASSOCIATED POLICIES

- Information governance policy.
- Information security policy.
- Freedom of Information policy.
- Knowledge and information management (KIM) policy.
- Code of Practice on Confidential Personal Information

INFORMATION SECURITY POLICY

PURPOSE
The Information Security Policy ("The Policy"), and the Information Security Standards ("the Standards") that sit under it, detail the high-level security principles for General Practice Solutions and establish the framework under which each of the Standards should be interpreted, managed and applied. These documents have been produced in line with the requirements and guidance contained in ISO27001 and ISO27002:2005.

The overall purpose of the Policy is to provide an overview of GPS information security requirements. The overall purpose of the Standards is to provide a detailed reference document which may be used to address specific queries on information security.

The Policy and Standards apply, and will be available to, all workers at GPS in whatever capacity. They are also relevant as evidence of established information security practices during internal or external audit processes. Relevant sections of the Policy and Standards may also be used as a reference point in negotiating or agreeing contracts with external suppliers.

The measures and controls detailed within the Policy and Standards set the security goals within GPS in line with the security strategy to achieve compliance with ISO27001. To this end the policy details the intention of GPS to comply with the ISO standard, it does not provide a summary of the current state of security controls in place at any given time.

The purpose of detailing the ISO27001 compliant controls in this policy document is to set the standard that GPS aims to achieve and to provide the detail required by the business units and, where applicable, 3rd party suppliers to ensure that both existing and planned systems comply, or work incrementally towards compliance with, ISO27001.

IRP: October 2022

SCOPE
The Policy and Standards have been developed for use across the whole of GPS and comply with the requirements of widely recognised good information security practice. They will:

- Assist workers to apply the correct level of security control to their day-to-day activities in line with good practice and applicable regulation and legislation.
- Assist with the development and commissioning of new processes and systems by detailing the required security settings and standards.
- Be formatted, controlled, and distributed in line with GPS requirements.

The Policy and Standards will be available, as the correct up to date version, on the intranet to all workers.

Any departments or workers who have a requirement to store or otherwise use hard copies of the Policy and Standards should ensure that they frequently check that they have the latest version of the policy and refer any queries to the information security team. They should also ensure that any old, outdated versions of this document are destroyed and replaced as necessary.

IRD: October 2022

POLICY STATEMENT
As a consultancy service in England, GPS aims to demonstrate the same standards of information security as we expect the services that we provide guidance too.

THE IMPORTANCE OF INFORMATION SECURITY
Information can be defined as useful data for a particular analysis, decision or task. Information must always be protected appropriately irrespective of how it is stored, presented or communicated.

The main aims of information security are to preserve:

Confidentiality: ensuring that information is accessible only to those who are authorised to have access.

Integrity: safeguarding the accuracy and completeness of information and processing methods.

Vailability: ensuring that authorised users have access to information when needed.

It also aims to support the requirements:

Accountability: accounting for the actions of individuals by monitoring their activities.

Non-Repudiation: legally acceptable assurance that transmitted information has been issued from and received by the correct, appropriately authorised, individuals.

GPS has a responsibility to securely manage its information assets, the information made available to it by providers and the people who use our client providers' services, as well as that provided by its own employees, contractors, and business partners. GPS has a responsibility to protect that information from unauthorised disclosure, loss of integrity or loss of availability.

All parts and agents of the organisation are responsible for making sure that information is protected adequately in accordance with the Policy and Standards.

GPS recognises the sensitive nature of the information that the organisation holds and processes, and the serious potential harm that could be caused by security incidents affecting this information.

GPS will therefore give the highest priority to information security. This will mean that security matters will be considered as a high priority in making any business decisions. This will help ensure that GPS will allocate sufficient human, technical and financial resources to information security management, and will take appropriate action in response to all violations of Security Policy.

GPS will use this Security Policy and the Standards as the basis for an organisation-wide strategy to set the correct level of information security.

The security efforts will be:

Coordinated: security measures will be based on a common framework provided by the Policy and Standards, and all workers will be involved in maintaining compliance with the security policy.

Proactive: we will detect, identify and manage vulnerabilities, threats, and security gaps to prevent security incidents as far as we possibly can.

Supported at the highest level: senior management are actively committed to information security and give their full support to implementing the required security controls that are identified through a continuous risk assessment process.

These security efforts will be structured and directed by the Security Policy, which covers all aspects of information security within GPS's business operations.

IRD. October 2022

RESPONSIBILITIES

PARTY	KEY RESPONSIBILITIES
All workers (including those in the roles below)	All staff will adhere to this Policy and the Standards. They will raise any issues of non-compliance, information risk or incidents with their line manager and the security team.
The Chief Executive Officer (CEO) and the Board of Directors	Ensuring that systems are in place to support appropriate information security measures.
Senior Information Risk Owner (SIRO)	Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of GPS are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with GPS's legal, statutory and organisational requirements.' (GPS, Corporate Governance Framework). See also Scheme of Delegation.
Information Governance Group	Approval, review and oversight of The Standards. Oversight, guidance and approval of the information risk and incident management processes. Providing advice to the GPS Executive team, via the SIRO, on policies, systems, guidance, methodologies, and training for information security.
Information Security Manager	Definition, implementation, monitoring and management of the Information Security Management System (ISMS) and information security policy documents. Organisation, management, and participation in any joint information security committees with the Department of Health, 3rd party ICT providers and other external organisations.
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: Inform and advise on compliance with data

ERD: October 2022

	protection law. Monitor compliance with data protection law. Provide advice as regards data protection impact assessments. Cooperate with the ICO. Act as contact point with the ICO on issues relating to processing. To carry out these tasks with due regard to risks relating to the processing of personal data.

LRD: October 2022

MONITORING COMPLIANCE

Monitoring compliance and effectiveness of the Policy and Standards will be carried out in several ways:

The Information Security Manager will provide reports on compliance with the Policy and Standards, when appropriate, using measures agreed with the ET and IGG. These reports will be presented to the DPO, Caldicott Guardian and SIRO at IGG meetings and key issues of compliance and performance will be reported to ET.

Review of effectiveness during the information and compliance status reviews, which are part of the annual Data Security Toolkit submissions

External audits commissioned in line with Department of Health and Social Care directives to check compliance with recognised security standards.

Internal, targeted audits of specific information security areas. These will be triggered by the risk management process, incident management or areas of concern highlighted by workers or senior management of GPS.

All compliance monitoring, audits and reporting will be included on the agenda of the IG Group meetings and minutes along with any actions and responsible owners.

ASSOCIATED POLICIES

- Information governance policy.
- Data Protection policy.
- Freedom of Information policy.
- Knowledge and information management (KIM) policy.
- Code of Practice on Confidential Personal Information.

CYBER SECURITY POLICY

INTRODUCTION
This policy is to ensure GPS workers applies Information Governance guidelines on cyber security, including implementing a robust defence against and reporting attempted cyber-attacks, and being aware of the dangers of systems being infected by malicious software (malware). These measures are put in place to protect information assets, such as client provider and patient records.

Cyber Attacks
Cyber attacks are an increasing threat, in terms of their growing sophistication and the scale of the detrimental impact they can cause. One of the main methods for such an attack is the sending of unsolicited emails that have been specifically designed to trick users into clicking links or opening attachments that will result in malware being downloaded to their system. The practice will guard against weaknesses in system configurations and promote staff working practices that guard against cyber attacks.

Malware
Malware is commonly defined as any software that is hostile or intrusive, and includes computer viruses, worms, Trojan horses, ransomware, spyware, adware and other malicious programs.

The practice sets out the following controls to address the risk posed by malware in terms of reduced integrity and availability of its information assets:

- All software installed on organisational assets is to be appropriately licensed.
- The [*IT manager or equivalent – please insert name/role as appropriate*] must authorise any installation of software.
- The [*IT manager or equivalent – please insert name/role as appropriate*] is responsible for the installation and regular update of anti-virus software on all appropriate machines (servers and clients).
- All media is to be virus-checked before being used.
- Procedures for reporting and handling virus attacks and recovering from them to be implemented, including immediate reporting of any suspicion of virus.
- Awareness of malicious 'hoax' attacks and procedure for handling them, including reporting to [*IT manager or equivalent – please insert title as appropriate*].

Staff members being made aware of the above controls, and the responsibilities arising from them, is of primary importance to the practice. Staff remaining vigilant to the threats of malware is essential in ensuring that only licensed software is used and that suspicious email attachments are dealt with appropriately.

Dealing with Cyber Attacks
In the event of a cyber-attack, the practice will limit the damage caused by an attack and reduce the time it will take to recover, as well as the costs involved, by having plans in place to:

- Isolate the incident.
- Make timely and effective repairs to hardware and systems where necessary.
- Recover any data that has been compromised.

Password Management
Passwords should be strong and secure, changed on a regular basis and not shared with others. Passwords used for personal email accounts etc. should not be the same the same as ones used for practice-based accounts. Where it is suspected that a password has been compromised, it should be changed immediately.

IRD: October 2021

Reporting Serious Incidents
All incidents will be investigated immediately and reported using the Significant Incident procedure in a timescale appropriate to the initial risk assessment. Reports and recommendations will be approved and monitored by the practice's Information Governance Lead, who will escalate as appropriate. See also, Significant / Critical Event Toolkit [*].

Resources
Computer and Data Security Procedure
Information Governance - Statement of Compliance Version 12
Common Cyber Attacks: Reducing the Impact
Cyber Essentials Scheme: Overview
Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks.

LRD: October 2022

LRD: October 2022