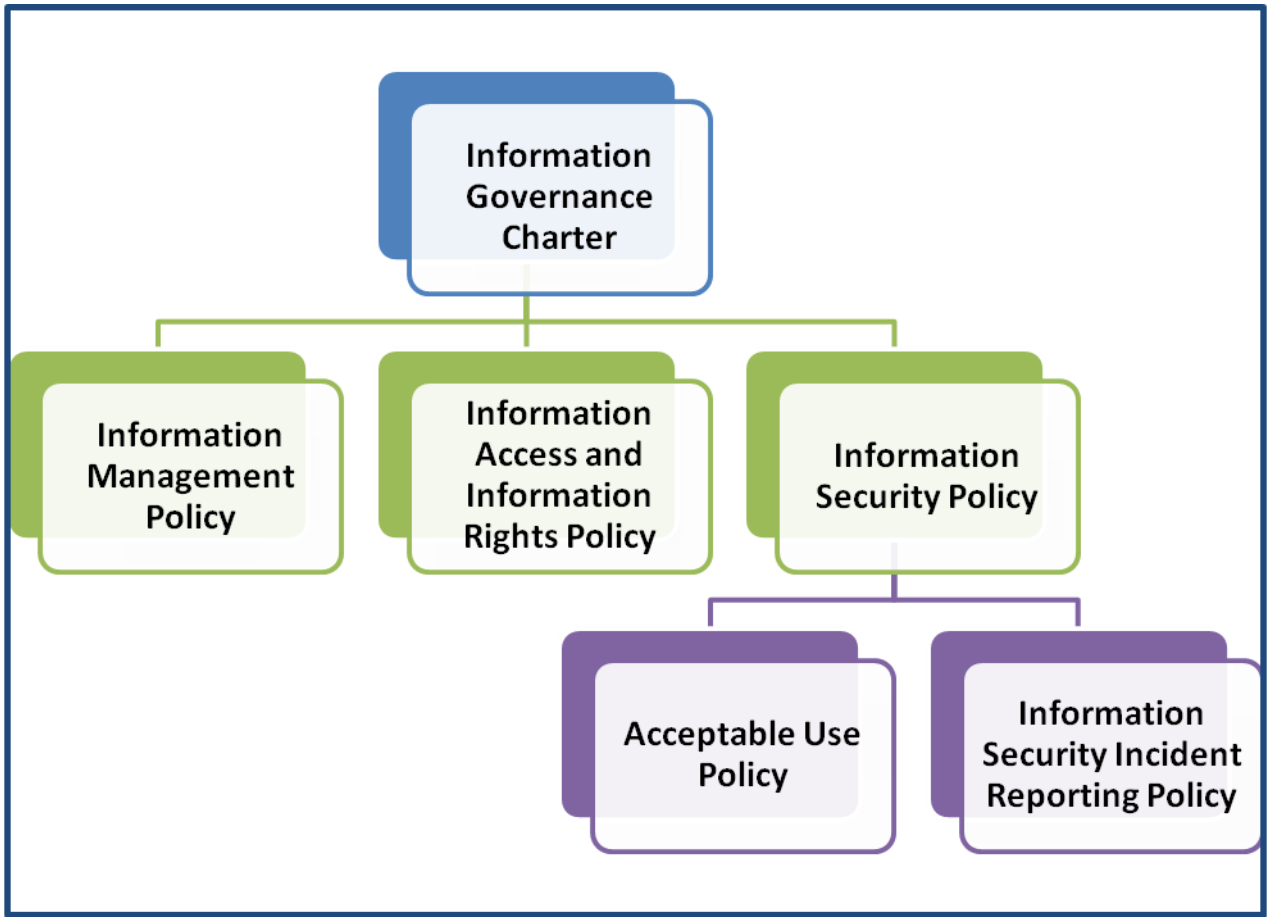
Dr Ingram & Partners

Information Governance Policy Suite

Publication Date:	24th May 2018
Version	1.0
Last Updated:	23rd May 2018
Next Review Date:	May 2019

Document Contents

Policy Framework



Information Governance Charter

Dr Ingram & Partners is committed to maintaining excellent information governance standards, protecting the personal data of its patients, and utilising personal data, in a safe and secure manner, for the benefit of the patient, the local community, and the wider health sector. This charter is Dr Ingram & Partner's promise to uphold these expected standards at all times.

1. Dr Ingram & Partners will produce and maintain a suite of information governance policies that will document how the Practice will adhere to the Data Protection Principles, Data Protection Legislation, and associated Codes of Practice.

2. Dr Ingram & Partners will maintain the standards set out in the NHS Information Governance Toolkit and will complete the Toolkit's assessment on an annual basis.

3. Dr Ingram & Partners will only disclose personal data to another organisation if it has a lawful and justified reason for doing so. Dr Ingram & Partners will not sell the data of its patients, employees, or other associates under any circumstances.

4. Dr Ingram & Partners will operate in a transparent and open manner so that its data subjects should not be surprised by how the Practice processes personal data.

5. Dr Ingram & Partners will maintain an adequate and robust information security framework and shall work towards achieving a Cyber Security Certificate.

6. Dr Ingram & Partners will put the data subject at the centre of all of its data processing activities and will ensure that the rights of the data subject are embedded in the culture of the Practice.

Dr Ingram & Partners

Jill Hillam
Practice Manager
24 May 2018

Information Management Policy

1.0 Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Dr Ingram & Partners programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Information Management Policy stipulates how the Practice will manage information effectively so that it can both benefit from the information it uses whilst at the same time ensuring that the information is used responsibly and securely.

This policy should be read in conjunction with the other policies in the Practice's Information Governance policy framework.

2.0 Scope

All policies in Dr Ingram & Partners Information Governance policy framework apply to all Practice employees, any authorised agents working on behalf of the Practice, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

3.0 Roles and Responsibilities

Senior Information Risk Owner (SIRO)

The SIRO is responsible for the Practice's overall information governance strategy and will be responsible for appointing the Data Protection Officer, and the Specific Point of Contact

(SPoC) The SIRO is accountable for the Practice's compliance with information governance legislation.

Caldicott Guardian

The Practice's Caldicott Guardian will ensure that the Practice uses the personal data of its service users legally, ethically, and appropriately whilst ensuring that confidentiality is maintained. The Caldicott Guardian will ensure that the Practice satisfies the highest practical standards when handling personal data.

Data Protection Officer (DPO):

The DPO is a statutory position and is the point of contact for the Information Commissioner's Office (ICO) and data subjects. The DPO will facilitate a periodic review of the corporate information asset register and information governance policies, assist with the reporting and investigation of information security breaches, and will provide advice on all aspects of data protection as required - in particular data protection impact assessments and information sharing agreements.

Specific Point of Contact (SPoC):

The SPoC is responsible for overseeing the Practice's day to day information governance strategy and in particular will coordinate the Practice's information security incident reporting process.

The current individuals with these responsibilities are:

Senior Information Risk Owner (SIRO)	Dr A J Ingram Senior Partner 01765692337
Caldicott Guardian	Dr J Pears GP Partner 01765692337
Specific Point of Contact (SPoC)	Jill Hillam Practice Manager 01765698731
Data Protection Officer (DPO)	Veritau Ltd Data Protection Officer 01609 53 2526

4.0 Data Quality

The Practice is committed to the collection and use of high quality data which is 'right first time' and can be relied upon for decision making and performance review. Data quality not only refers to numbers and statistics but also includes other information that the Practice may process. Names, addresses and other types of information must be recorded accurately in manual and electronic systems.

There are six key characteristics of good data quality as follows:

Accuracy	Data should be sufficiently accurate for its intended purposes, representing clearly and in sufficient detail the interaction provided at the point of activity. Data should be captured once only, although it may have multiple uses. Accuracy is most likely to be secured if data is captured as close to the point of activity as possible. Reported information that is based on accurate data provides a fair picture of performance and should enable informed decision making at all levels. The need for accuracy must be balanced with the importance of the uses for the data, and the costs and effort of collection. For example, it may be appropriate to accept a lower degree of precision where timeliness is important. Where compromises have to be made on accuracy, the resulting limitations of the data should be clear to its users.
Validity	Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions. This will ensure consistency between periods and with similar organisations. Where proxy data is used to compensate for an absence of actual data, organisations must consider how well this data is able to satisfy its intended purpose.
Reliability	Data should reflect stable and consistent data collection processes across collection points and over time, whether using manual or computer-based systems, or a combination. Managers and stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or methods.
Timeliness	Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence the appropriate level of service or management decisions.
Relevance	Data captured should be relevant to the purposes for which it is used. This entails periodic review of requirements to reflect changing needs. It may be necessary to capture data at the point of activity which is relevant only for other purposes, rather than for the current intervention. Quality assurance and feedback processes are needed to ensure the quality of such data.
Completeness	Data requirements should be clearly specified based on the information needs of the organisation and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

5.0 Data Risks

One of the objectives of the Practice's information governance strategy is to ensure the confidentiality, integrity and availability of information held by the Practice by reducing the risk of:

- Unauthorised access to data,

- Incomplete or inaccurate data,
- The unnecessary use of data;

Information risk management is the process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

Risks can never be eliminated fully. A structured, systematic and focused approach to managing risk is therefore required. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some degree of risk taking is inevitable and necessary if the Practice is to achieve its objectives. By being 'risk aware', the Practice is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

6.0 Information Asset Management

In order for the Practice to effectively manage the information that it holds and the risks associated with that information, it maintains an information asset management system.

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected, and exploited effectively. Information Assets have recognisable and manageable value, risk, content, and life cycles.

Information Asset Register

The DPO will assist the Practice in developing and maintaining a corporate information asset register. The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format, location, and retention of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset
- Risk rating;

The register will be reviewed annually and Information Asset Owners will inform the DPO of any changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (IAO) is a Practice employee who is responsible for an information asset, understands the value of that information and the risks associated with it. The IAOs will be identified by the SIRO and DPO.

IAOs are responsible for ensuring the security and maintenance of their information assets. This includes ensuring other officers are using the information responsibly and safely. The role also includes determining the retention period for the asset and ensuring the information is securely destroyed in accordance with this period.

7.0 Retention and Destruction of Records

As well as maintaining an Information Asset Register the Practice will also maintain a Retention and Destruction Schedule so that (a) it understands the retention requirements for all of the information it holds and (b) it is able to identify if and when a record was destroyed.

Retention Periods

Retention periods will be determined by any legal requirement, any best practice or national guidance, and lastly the business need to retain the information.

In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

Destruction of Records

When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins.

A record should be retained of all files destroyed which includes, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record,
- Authorising IAO;

In exceptional cases upon reaching the end of its retention period an IAO may consider it necessary to assign a new retention period for that individual record, for example regulatory involvement may necessitate records being kept for longer than usual.

8.0 Information Sharing

In order to operate efficiently and provide the optimum service to service users it is sometimes necessary to share personal information with other Data Controllers. Routine and regular information sharing arrangements will be documented in an information sharing agreement. The Data Protection Officer is required to advise on all information sharing agreements, will provide an adequate Information Sharing Agreement template, and will keep a register of completed information sharing agreements.

All information sharing agreements and any adhoc information sharing will be authorised by the appropriate information asset owner. All disclosures of information should be accurately recorded. Officers should take care to record when and how information is disclosed to other organisations.

9.0 Third Party Data Processors

All third party contractors who process data on behalf of the Practice must be able to provide assurances that they have adequate data protection controls in place to ensure that data that they process, on behalf of the Practice, is secure.

The Practice will include data processor clauses in all contracts with Data Processors. This will ensure that all arrangements are appropriately documented and that adequate safeguards are in place to ensure the processor is only using the personal data it is provided for the stipulated purpose(s).

The SIRO may insist that any data processing, by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place.

If any data processing is going to take place outside of the European Economic Area then the Data Protection Officer must be consulted prior to any contracts being agreed. The DPO may insist on stricter terms and conditions being included within the contracts to ensure personal data is kept secure and processed lawfully.

10.0 Data Protection Impact Assessments

The Practice will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks.

The IAO is responsible for ensuring the completion of the DPIA. The DPO must advise on such assessments.

High risk data processing projects where it is not possible to mitigate the risks to an acceptable level may require authorisation from the Information Commissioner's Office (ICO). The DPO will advise where this is the case and will liaise with the ICO, following consultation with the SIRO.

The DPO will keep a register of completed assessments and ensure that officers have access to a current assessment template.

11.0 Privacy Notices

The Practice will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. A corporate privacy notice will be displayed on the Practice's webpage in an easily accessible area. The notice will also be available in hard copy for those who request it. A hard copy will also be included within the Practice's admissions bundle.

Where possible, data subjects will be provided with a privacy notice before their data is obtained by the Practice. If this is not possible then it will be provided to the data subject as soon as possible after the Practice has obtained their data.

Privacy notices should be cleared by the DPO prior to being published. A record of privacy notices shall be kept on the Practice's Information Asset Register.

12.0 Training

The Practice will provide basic training to all employees so that every employee is aware of the practice's responsibilities under Data Protection legislation. This includes all temporary staff.

Basic training will be undertaken prior to any individual being given access to Practice systems or personal information. Advanced training will be given to employees who are expected to collate requested information and respond to requests for information.

Information governance training will be renewed annually for employees.

The Practice will also insist that third party contractors ensure their employees are adequately trained in information governance.

The SIRO is responsible for ensuring the training resources are effective and training requirements are adhered to.

Information Access and Information Rights Policy

1.0 Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Practice Name's programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Information Access and Information Rights Policy stipulates how the Practice will deal with requests for personal information, known as a Subject Access Request, and requests to exercise data protection rights enshrined by law.

This policy should be read in conjunction with the other policies in the Practice's Information Governance policy framework.

2.0 Scope

All policies in Dr Ingram & Partners Information Governance policy framework apply to all Practice employees, any authorised agents working on behalf of the Practice, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

3.0 Requests for Information under the Freedom of Information Act 2000 (FOI) and Environmental Information Requests 2004 (EIR)

Freedom of Information (FOI) requests generally applies to all information held by the Practice subject to certain exemptions. FOI does not generally apply to private correspondence of employees. Environmental Information Regulations (EIR) requests apply to all environmental information held by the Practice subject to certain exemptions.

In line with Schedule 1 Part III (Clause 43A) of the FOI Act, requests can only be made, to Practices, in relation to the provision of Primary Medical Services.

The coordination of the FOI process is the responsibility of the Practice Manager. The responsibility includes:

- Deciding whether the information requested is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester.

Receiving a Request

Any employee of the Practice could receive a request for information. When such a request is received it should be passed immediately to the customer service centre for processing.

Each request received by the Practice will be acknowledged with the applicant within 5 working days by the Practice Secretary**.**

The Practice Manager will log the request, provide a reference number and forward the request onto the responsible employee to respond. EIR requests do not need to be submitted in writing and can be submitted orally. However the receiving employee should write this request down for the responsible officer to confirm in writing the details of the request with the applicant.

Timescales and Fees

The Practice Manager is responsible for compliance with FOI/EIR timescales.

The circumstances under which the Practice may impose a charge are extremely limited. Any charges will be imposed in accordance with the Practice's charging regime.

Searching for Information

When locating information across Practice filing systems, databases, and archives (electronic and manual) employees should take care to search variations of file names.

Employees should make a record of what search terms they used and what systems were searched.

Exemptions

There are a range of exemptions and exceptions, both in FOIA and EIR, which may be applied to intended disclosure. Often these exemptions are subject to the public interest test where the responsible officer must decide if it the public interest in withholding the information outweighs the public interest in disclosing the information. If the responsible employee is of the opinion that an exemption may apply, he or she should seek advice from their legal advisers or the Data Protection Officer before withholding the information.

Responding to Requests

Applicants are able to request hard copies of the information or electronic copies of the information. The Practice is not obliged to comply with a particular format unless it is reasonable to do so. All responses will be sent electronically where possible.

Where copy documents are requested there is no requirement to send a copy of the document to the applicant. In some cases it may be easier to extract the information from the document or to provide a digest.

Employees should take care to ensure redactions are permanent and cannot be reversed.

When responding to any request which is potentially sensitive or controversial the responsible employee will consider where any additional senior management approval might be required prior to responding to the request.

Publication Scheme

The Practice will adopt the Information Commissioner's model publication scheme.

The publication scheme will be maintained by the Practice Manager and reviewed on an annual basis.

Prospective FOI/EIR applicants will be advised to refer to the publication scheme prior to submitting a request for information.

4.0 Requests for Information under Data Protection Act 2018 (Subject Access Requests)

The Data Protection Act (DPA 2018) gives data subjects the right to access their own information that the Practice holds about them. This is known as a Subject Access Request (SAR).

Receiving a Request

Any employee of the Practice could receive a request from an applicant at any time.

The DPA 2018 does not require subject access requests to be made in writing. However, applicants will be encouraged to complete the 'Subject Access Request Form' where possible, to ensure that all necessary information is required.

Requests that are received orally will be written down by the receiving employee and confirmed with the applicant to ensure the Practice understands the applicant's request. All requests for personal information must be passed to the Practice Secretary who will log on the Practice's corporate register and assign a reference number. The Practice Secretary will be responsible for responding to the request.

The Practice must be satisfied as to the applicant's identity. If the responsible officer is not certain of the applicant's identity from existing Practice records or involvement with the applicant, they may ask that that applicant produce:

- Valid Photo ID (driver's licence, passport etc),
- Proof of Address (Utility bill, council tax letter etc),
- Or enough information for the Practice to be satisfied of the applicant's identity;

Timescales and Fees

A request only becomes valid once the Practice is satisfied it has sufficient detail to respond to the request; it has 30 calendar days to respond.

The Practice can apply a discretionary extension of up to 60 calendar days to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either complexity of the case or volume of the information. If the Practice wishes to apply an extension they will inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads.

In very limited cases the Practice may also refuse a request outright as 'manifestly unreasonable' if the Practice would have to spend an unjustified amount of time and resources to comply. Employees should consult with the Data Protection Officer prior to applying this refusal.

No fee may be charged for processing a request. However, charges can be applied if an applicant is requesting a duplicate copy of information that has already been supplied to them under a previous request. Charges should follow the Practice's charging schedule which can be found in Appendix One of this Policy.

Fees will still be charged for requests for the creation of medical reports or doctor's opinions where new information is being created and therefore do not fall under the scope of Subject Access. Fees will be charged according to the charging schedule in Appendix One.

Searching for Information

When locating information across filing systems, databases, and archives (electronic and manual) employees should take care to search name variations, initials, and nicknames. Employees should make a record of what search terms they used and what systems were searched.

Exemptions and Third Party Information

There are a range of exemptions, in the Data Protection Act, which can be applied to some or all of the information being requested. A data subject's right to their own data is very strong and the Practice will only apply exemptions when absolutely necessary.

Third Party data, that is data about a person other than the data subject, should also be withheld from the disclosure unless:

- The third party individual has given consent;
- They are incapable of giving consent; or
- There is a reasonable expectation of disclosure (i.e the third party is a Practice employee or other professional working with the data subject);

Responding to Requests

Subject Access Requests must be answered within the timeframes stipulated above.

The Practice is obliged to send responses in the same format as the request was received – every effort will be made to comply with this requirement. If an applicant requests the information in a specific format the Practice is not obliged to comply unless it is reasonable to do so. In some cases it may be easier to extract the information from the document or to provide a digest.

Employees should take care to ensure redactions are permanent and cannot be reversed.

5.0 Other Rights of the Data Subject

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR and Data Protection Act 2018:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the Secretary who will acknowledge the request, log the request on the central register and assign a unique reference number. The Secretary will ensure the request is responded to within 30 calendar days.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Employees should refer to the DPO and the Caldicott Guardian if there are any complex issues in regards to the above requests.

6.0 Data Protection Complaints

The DPA 2018 does not have a statutory internal review mechanism. However, it is considered best practice for organisations to have a complaints procedure.

Therefore, any complaints about subject access requests should be directed to the Practice Manager who will respond to the applicant within 30 calendar days.

Information Security Incident Reporting Policy

1.0 Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Dr Ingram & Partners programme to comply with the new legislation it has written a new suite of Information Governance policies.

An information security incident can be defined as any incident that has breached the Practice's information security framework. This will generally be a breach of data confidentiality (i.e. unauthorised access), data integrity (i.e. incorrect or outdated data), or data availability (i.e. accidental loss or destruction).

Article 33 of the GDPR compels data controllers to report information security incidents to the Information Commissioner's Office (ICO), within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that the Practice has a robust system in place to manage, contain, and report such incidents.

The Information Security Incident reporting policy specifically outlines the Practice's duty to report an information security incident and details how the Practice will achieve this.

2.0 Scope

All policies in Dr Ingram & Partners Information Governance policy framework apply to all Practice employees, any authorised agents working on behalf of the Practice, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,

- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

3.0 Incident Discovery and Containment (Within 24 Hours)

If an employee, or Practice associate, is made aware of an information security incident, or potential information security incident, then they must report it to the Practice Manager within 24 hours. If the Practice Manager is not at work at the time of the notification then their Out of Office email will nominate another individual to start the investigation process.

If appropriate, the individual who discovered the incident, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

4.0 Initial Investigation (Within 48 Hours)

Once received, the Practice Manager will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

WHITE	*Near Miss Incident* No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
GREEN	*Minimal Impact Incident* A breach of confidentiality, integrity, or availability has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.
AMBER	*Moderate Impact Incident* The Practice's security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office. The data disclosed does not contain any 'Special Categories'* of data.
RED	*Serious Impact Incident* A breach of security involving special category* data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.

	*Special Categories of Data include: Details about mental or physical health, Details about sexual orientation or sexual activity, Details about race or ethnicity, Details about religious or philosophical beliefs, Details about political affiliation or beliefs, Details about Trade Union membership, Biometric or Genetic Data, Details about criminal conviction history.

The Practice Manager will notify the Senior Information Risk Owner (SIRO), the relevant Information Asset Owner (IAO), and the Caldicott guardian that the breach has taken place. The above individuals will recommend immediate actions that need to take place to contain the incident. Where the incident is considered to meet the 'Red' threshold then the Practice Manager will also inform the Data Protection Officer (DPO) who will offer advice about containment, recovery, and reporting.

5.0 Incident Reporting (Within 72 Hours)

The SIRO, in conjunction with the Practice Manager, IAO and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed of the incident. The SIRO will be ultimately responsible for this decision.

The Practice Manager or IAO will be responsible for liaising with data subjects. The DPO will be responsible for liaising with, and reporting to, the ICO.

The Practice is also required to log the incident on the NHS's *Significant Incidents Log.* The Practice Manager will be responsible for doing this.

6.0 Investigating and Concluding Incidents

The Practice Manager will investigate white, green and amber incidents. Red incidents will be investigated by the DPO with the assistance of Internal Audit and Counter Fraud Teams.

The SIRO will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the Practice.

7.0 Recording Incidents and Monitoring Incident Trends

The Practice Manager, will be responsible for maintaining a central record of information security incidents. This record will state the following:

- Nature of Incident,

- Date of Incident,
- Categories of Personal Data,
- Likely Harm or Detriment,
- Incident Threshold Rating,
- Investigation Officer
    - Investigation Conclusion Date
    - Investigation Outcome
    - Date signed by SIRO
- Reportable to the ICO?
    - Date reported to ICO
    - ICO Response Date
    - ICO Outcome
- Reportable to the Data Subject?
    - Date reported to Data Subject
- Notes

This record will be used by the Practice to identify any incident trends, for example where the same incident has occurred over a short period of time.

The DPO will use the record as part of their investigation should a 'Red' incident occur.