Information and Data Protection Policy

Directorate:	**Corporate Governance and Compliance**		
Lead Officer:	Director of Corporate Governance and Compliance		
Approved by:	Angelo Fernandes		
Approval Date:	27/5/22	Review Date:	27/5/23

Change History

Version	Date Issued	Originator/Modified by	Reason for Change
1		Angelo Fernandes	First release
2		Angelo Fernandes/Duncan Smith	Annual review/Brexit update
2.01		Angelo Fernandes/Duncan Smith	Role responsibility clarification DRAFT
2.02		Angelo Fernandes/Harjit Sandhu	Note re clarity from Ethical IT on vCISO
2.03		Angelo Fernandes	Expanded 1.2 section to acknowledge risk and due diligence.
2.04		Angelo Fernandes	Modified 6.2 to include “Availability, Integrity and Confidentiality”
2.05		Duncan Smith	Policy reformatted and table of relevant documents added as appendix
3.0		Duncan Smith/Angelo Fernandes/CQC Compliance Ltd	Review, re-draft and reposition as part of the Response information governance strategy and formal requirement for NHS DSPT.

1. INCLUSIVITY

1.1 If you require assistance to read or understand this policy, please let your manager or HR know as translation, interpretation, Braille or a signing service can be made available.

2. POLICY STATEMENT AIMS AND PRINCIPLES

2.1 This policy is part of our wider Information Governance strategy which establishes the governance structure, procedures and protocols we will follow to ensure that our activities and technologies that we employ maximise the value of ALL information while minimising associated risks and costs and assuring compliance with relevant legislation and contractual obligations. This strategy includes our Information and Data Protection Policy.

2.2 This policy establishes the governance structure, procedures and protocols we will follow to ensure that we meet our legal and contractual responsibilities to demonstrate that Response is accountable for all its activities in relation to **the processing of Personal Data and Personal Confidential Data**. This includes compliance with specific contractual obligations, e.g., the NHS Data Security Protection Toolkit (DSPT) and its 'Information Governance' requirements.

2.3 This Policy gives assurance to data subjects, including members of staff, individuals, clients that personal data is dealt with legally, securely, efficiently and effectively to deliver the best possible care and support. It encompasses both data protection and information security.

3. SCOPE

3.1 This policy applies to all people, properties, activities, and functions undertaken by, or on behalf of, the organisation and applies to all employees, contractors and anybody who is or may be impacted upon by our work activities (Data Users).

4. DEFINITIONS

4.1 **Controllers** are the people who, or organisations which, determine the purposes for which, and the way any Data is processed. They have a responsibility to establish practices and policies in line with relevant laws. We are the Data Controller of all Data used in our organisation.

4.2 **Criminal Offence Data** is Data which relates to an individual's criminal convictions and offences. It can only be processed under

strict conditions and may require the explicit consent of the person concerned.

4.3 **Data Breach** is any act or omission which compromises the security, confidentiality, integrity or availability of Data, or the safeguards that we or a third party put in place to protect the Data, including losing the Data or disclosing it to unauthorised people. In the event of a data breach, the data breach procedure must be followed.

4.4 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Data.

4.5 **Data Users** include employees and contractors whose work involves using Data on behalf of Response. Data Users have a duty to protect the Data they handle by always following our data protection and security policies. All Data Users have a responsibility, when using Data, to comply with any security safeguards and procedures we put in place.

4.6 **Personal Confidential Data** is a term used in the Caldicott Information Governance Review and refers to personal information which should be kept private or. This definition includes data relating to the deceased as well as living people, and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and includes special category data as defined in the Data Protection Act.

4.7 **Personal Data** as defined in the Data Protection Act 2018, is information which relates to a living individual who can be directly or indirectly identified from that information. Data can be factual (such as a name, address, or date of birth) or it can be an opinion (such as a performance appraisal).

4.8 **Processing** is any activity that involves use of Data. It includes obtaining, recording, holding, or carrying out any operation or set of operations on Data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Data to third parties.

4.9 **Processors** include any people who, or organisations which, process Data on behalf of a controller. Employees of Response are excluded from this definition, but it could include third party suppliers which handle Data on our behalf.

4.10 **Special Categories of Data** are sensitive categories of Data about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health

or condition, sexual life, or sexual orientation. It also includes genetic and biometric Data (where used for ID purposes). Special Categories of Data can only be processed under strict conditions and may require the explicit consent of the person concerned.

4.11 **vCISO** is the virtual Chief Information Security Officer. This role may be contracted to a third party.

5. COMPLIANCE

5.1 This Policy has been created to,

5.1.1 meet the legal requirements as stated in the following legislation:

a) Data Protection Act 2018 (Data Protection Act or DPA)
b) UK General Data Protection Regulation ('GDPR')

5.1.2 meet our contractual obligations for the processing of personal data and personal confidential data commissioned by the NHS or authorised commissioning body, including the requirements as set out in the NHS Data Security Protection Toolkit (DSPT).

6. DELEGATION AND RESPONSIBILITY

6.1 The executive team are responsible for ensuring this policy and the relevant statutory requirements are being met. Individual posts with specific responsibilities to manage will be identified within the Operating Procedures and Guidance Notes.

7. POLICY DETAIL

7.1 Response endorses the data protection principles set out in the GDPR. All Data Users must ensure that these principles, together with the requirements of the DPA, are followed. In summary, these state that personal data shall be.

a) Processed fairly, lawfully, and in a transparent manner. (Fairness, Lawfulness and Transparency)
b) Processed for specified, explicit and legitimate purposes and in an appropriate way. (Purpose Limitation)
c) Adequate, relevant, and limited to what is necessary for the stated purpose. (Data Minimisation)
d) Kept accurate and up to date (Accuracy)
e) Not kept longer than necessary for the stated purpose. (Storage Limitation)
f) Processed in a manner that ensures appropriate security of Data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, by using appropriate technical or organisational measures. (Availability, Integrity, Confidentiality)

g) Not transferred to another country without appropriate safeguards being in place. (Transfer Limitation)
h) Processed in accordance with Data Subjects' rights. (Data Subject's Rights and Requests)

7.2 Response is further committed to implementing the eight **Caldicott Principles** for handling patient-identifiable information, where 'patient' refers to our service user or resident, namely.

Principle 1: Justify the purpose(s) for using confidential information.

Principle 2: Use confidential information only when it is necessary.

Principle 3: Use the minimum necessary confidential information.

Principle 4: Access to confidential information should be on a strict need-to-know basis.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities.

Principle 6: Comply with the law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Principle 8: Inform patients and service users about how their confidential information is used.

7.3 Fair and Lawful Processing

7.3.1 Under the GDPR, data will be lawfully processed by Response under the following conditions,

- the consent of the data subject has been obtained
- processing is necessary for:
  - compliance with a legal obligation
  - the performance of a task carried out in public interest or in the exercise of official authority vested in the controller
  - for the performance of a contract with the data subject or to take steps to enter into a contract
  - protecting the vital interests of a data subject or another person
  - for the purposes of legitimate interests pursued by the controller or a third party, except where such interests

are overridden by the interests, rights or freedoms of the data subject.

7.3.2 Response will obtain the explicit consent of the individual concerned for all processing of special category data, unless,

7.3.2.1 it is information relating to racial/ethnic origin, disability or religious belief that is being collected purely for monitoring equality of opportunity or treatment

7.3.2.2 it relates to the employment of individuals

7.3.2.3 it is necessary for the provision of advice or support and the data subject cannot reasonably be expected to give explicit consent.

7.4 **Management of Data Processors**

7.4.1 Response will require all data processors to formally agree that personal data will not be used for any purpose other than that agreed. Response will not disclose personal data to third parties, unless:

7.4.1.1 carrying out obligations under employment, social security or social protection law or a collective agreement

7.4.1.2 protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

7.4.1.3 the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

7.4.1.4 reasons of substantial public interest on the basis of Union or Member State law, which is proportionate to the aim pursued and which contains appropriate safeguards

7.4.1.5 the purposes of preventative or occupational medicine, for assessing the working capacity of the members of staff, medical diagnosis, the provision of health, social care, treatment, management of health, or social care systems and services on the basis of Union or Member State law or a contract with a health professional

7.4.1.6 reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

7.4.1.7 archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7.5 All disclosures of personal data to third parties must be authorised by a member of the Senior Management Team and be limited to the

minimum information required. All disclosures must be recorded either in the personnel or client's record.

7.6 Duties and responsibilities.

7.6.1 We take an open, transparent based approach to potential breaches of the legislation and encourage ALL staff to raise alerts and subsequently encourage personal and organisational learning.

7.6.2 However, where there is negligence, any breach of the DPA or GDPR with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with Response policy may be viewed as potential misconduct or gross misconduct and may result in disciplinary action being taken, up to and including dismissal. Employees could also face criminal proceedings.

7.7 Director of Corporate Governance and Compliance (DCGC)

7.7.1 The DCGC has overall responsibility for information governance including data protection within the organisation. The Director of CGC is supported by the Chief Executive Office, the CEO and the Director of Finance and Information to meet these requirements. The Director of Corporate Governance and Compliance also reports directly to the Chair of the Audit and Risk Committee on information governance.

7.7.2 The Head of Corporate Governance and Compliance will deputise for the DCGC when they are absent. The Head of Corporate Governance and Compliance will advise the DCGC of any decisions made in respect to information governance on the DCGC's return.

7.7.3 The DCGC has the following responsibilities.

a) reports on information risk and information governance to the Audit and Risk Committee (ARC)
b) makes the final decision in issues that arise regarding the protection and use of personal information.
c) receives and considers reports into breaches of data protection and where appropriate ensures remedial action is undertaken.
d) ensures there is a framework enabling Caldicott principles to be reflected in Response's policies and procedures for the management and use of personal information.

7.7.4 The DCGC will, on at least an annual basis, ensure the following.

a) Response has effective policies and management arrangements covering all aspects of information governance and information risk.

b) Response undertakes or commissions assessments and audits of its Information Governance policies and arrangements.

c) all information processed has a suitable lawful basis which is recorded in the record of processing activities (RoPA)

d) computerised and manual filing systems containing Personal Data must be documented in the Information Asset Register which forms part of the ROPA. The Asset Register will record:
   - the Service Area to which the entry relates
   - the name of the computer system, manual files or both in which the data is stored
   - whom the information is held about
   - what personal information is held, including any sensitive personal data that is being held
   - how the data is protected (e.g., restricted access or protected access)
   - retention period for the data
   - The Information Asset Owner

e) Privacy notices are in place and are up to date for all individuals for whom we store personal information.

f) Data Processing Impact Assessments are up to date and are in place where required.

g) Response publicises Subject Access Rights appropriately.

h) Data sharing agreements are in place for all organisations Response shares information with.

i) Liaise with other Response committees or groups to promote information governance and information risk issues.

j) Report to the ARC on information governance and information risk issues.

7.8 Director of Finance and Information

7.8.1 The Director of Finance and Information has overall responsibility for Information Security and Information Risk within the organisation. This has been delegated to Ethical IT acting as our virtual Chief Information Security Officer (vCISO). The Director of Finance and Information and the vCISO is supported by the Chief Executive Office, the CEO and the Director of CGC to meet these requirements.

7.8.2 The Director of Finance and Information supported by the vCISO has the following responsibilities.

a) reports on security and technical information risk to the ARC.

b) makes the final decision in issues that arise regarding security and technical information risk.

c) receives and considers reports into security related data breaches and where appropriate ensures remedial action is undertaken.

7.8.3 The Director of Finance and Information supported by the vCISO will, on at least on an annual basis, ensure the following.

a) Response has effective policies and management arrangements covering all aspects of information security and technical information risk.
b) Response undertakes or commissions assessments and audits of its Information Security policies and arrangements.
c) Data Processing Impact Assessments are up to date and are in place where required e.g. implementation of new/novel IT in liaison with the DPO.
d) Take ownership of the security and technical risk assessment process for information risk.
e) Review and agree action in respect of identified security and technical information risks.
f) Ensure that the organisation's approach to security and technical information risk is effective in terms of resource, commitment, and execution and that this is communicated to all staff.
g) Provide a focal point for the resolution and/or discussion of security and technical information risk issues.
h) Report to the ARC on security and technical risk issues

7.9 Data Protection Officer (DPO)

7.9.1 The core activities of Response include the large-scale processing of special category data. Accordingly, a DPO has been appointed.

7.9.2 The DPO will act as the "conscience" of the organisation regarding confidentiality and ensure that the organisation satisfies the highest practical standards for the handling of information, both within the organisation and data flows to other NHS and non-NHS organisations.

7.9.3 The DPO will work closely with the ARC and vCISO to achieve this standard. If Response decides not to follow the advice given by the DPO, Response will document its reasons to demonstrate accountability.

7.9.4 The DPO's tasks are, in addition to those mandated by GDPR.

a) Support the ARC to undertake its assurance tasks in relation to GDPR.
b) Offer organisational support and advice as required on matters of confidentiality and the safe use of information
c) To be the first organisation point of call where there is a data breach.
d) To establish learning where there is a data breach

e) Assist with the development of up-to-date policies and procedures in relation to data protection and ensure all other policies are compliant as appropriate.

f) Link into the Information Commissioner's Office and stay abreast of current legislation advising the Director of CGC accordingly.

g) Ensure the RoPA is maintained and kept up-to-date with the legally required information

h) Ensure compliance with contractual obligations, including the NHS DSPT.

7.9.5 The role of the DPO is currently assigned to the Director of CGC. It may in future be assigned to another member of staff or contracted to another organisation (third party).

7.10 Management (including Senior Management)

7.10.1 All managers will;

a) Ensure that all current and future staff are instructed in their duty of confidentiality and security responsibilities in liaison with the Head of HR and the Training Manager.

b) Ensure that staff understand protocols for obtaining, using, and disclosing personal information.

c) Ensure that no unauthorised staff or other staff can access any of Response's computer systems or manually held information.

d) Determine which individuals are to be given access to specific computer or manual systems. The level of access to specific systems should be on a job function need and independent of status.

e) Ensure that relevant system managers are advised about staff changes affecting computer access (e.g. job function changes or leaving a service/the organisation) in order that passwords may be disabled.

f) Monitor personal information to ensure that it is accurate and up to date.

g) Consult with the DPO where there is any significant query related to GDPR/information governance.

h) Report data breaches immediately using the designated system which will inform the relevant personnel e.g. Director Finance, Director CGC and DPO.

7.11 Data Users

7.11.1 All Data Users will;

a) comply with the requirements of the Data Protection Act and the Caldicott Principles.

Through appropriate training and responsible management, Data Users will.

a) Observe all guidance and codes of conduct in relation to obtaining, using, and disclosing personal information.
b) Observe all information sharing protocols in relation to the disclosure of information to provide care for individuals.
c) Obtain and process personal information only for specified purposes.
d) Only access personal information that is specifically required to carry out their work.
e) Record information accurately in both manual and electronic records.
f) Ensure that any personal information they hold is kept secure.
g) Ensure that personal data is not disclosed in any form to any unauthorised third party.
h) Ensure that any new process introduced ensures that confidentiality and data protection are considered.
i) Consult their manager in relation to any information governance/GDPR query.
j) Raise data breaches with the DPO.

7.12 Retention of personal information

7.12.1 Response will set retention periods for all personal data according to the data retention policy.

7.13 Access to personal information

7.13.1 In most cases, individuals are entitled to copies of personal information held about them (subject access). Subject access requests will be dealt with in accordance with the Access to Records procedures.

7.14 Security of personal information

7.14.1 Personal information will be held and transferred in a secure manner

7.15 Breaches of confidentiality or security

7.15.1 Any breaches of confidentiality or security will follow the data breach procedure. All incidents involving possible or actual breaches will be investigated. The DPO will be alerted and will inform the ARC.

7.15.2 Any breach or suspected breach of the GDPR must be reported immediately to the Data Protection Officer, providing as much information as possible. A breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever personal data is lost, destroyed, corrupted or disclosed, as well as if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable, for example, when it has been encrypted by ransomware or accidentally lost or destroyed.

7.15.3 The Data Protection Officer will investigate and, if appropriate, produce a report for the Senior Management Team. The Data Protection Officer will provide advice to the Senior Management Team on whether the breach requires notification to the Information Commissioner's Office (ICO). This advice should take account of the information provided on the ICO's website regarding the reporting of breaches.

7.15.4 The Data Protection Officer is required to notify the ICO of any breach that is likely to present a risk to the rights and freedoms of data subjects. If a decision is made not to report a breach to the ICO, the rationale must be documented so that it can be justified at a later date if required.

7.15.5 Response will ensure a record is kept of all data breaches as well as details of lessons learned. These will be shared throughout Response in line with the Incident Management Policy as well as themes and trends identified and acted upon.

7.15.6 The DPO will be alerted and will inform the Audit and Risk Committee of the number and severity of data breaches, as well as the number of ICO notifications, on at least a quarterly basis.

7.16 Collection and use of personal data

7.16.1 Information will only be collected and used for the following purposes.

a) Staff administration
b) Accounts and records
c) Provision and administration of safe support, care and housing to protect residents, service users and others
d) Research
e) Prevention of potential harm to an individual and prosecution of offenders
f) Public health

7.16.2 Response will only collect information that is necessary to carry out operational needs or to comply with legal requirements.

7.16.3 When collecting resident or service user data, service areas will ensure that individuals are adequately informed about the uses of

their information. All residents and service users will be provided with information which details.

a) The identity of the data controller
b) Purposes for using the information
c) How to obtain a copy of the information

7.16.4 When collecting other personal data e.g. staff data, Response will ensure that it is clear to the individual that their information is being processed by the organisation and the purposes for which it is being processed.

7.17 **Individual Rights – The Right to be Informed**

7.17.1 Response's privacy notice supplied to clients and members of staff regarding the processing of their personal data will be written in a clear, plain language, which is concise, transparent, and easily accessible.

7.17.2 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- the identity and contact details of Response and the Data Protection Officer
- the purpose of and the legal basis for processing the data
- the legitimate interest of Response (if applicable) or a third party
- any recipient categories of recipients of the personal data
- any international transfers of data
- how long the data will be stored for
- the existence of the data subject's rights, including the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

7.17.3 The privacy notice should also refer to any online information collated such as cookies. In relation to cookies, Response will:

- tell people the cookies are there
- explain what the cookies are doing and why

- get the person's consent to store a cookie on their device.

7.17.4 Fresh consent if may be required if the use of cookies changes over time.

7.18 Individual Rights – Subject Access Requests (SARS)

7.18.1 Individuals have the right to obtain confirmation that their data is being processed. They also have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

7.18.2 Response has a detailed Subject Access Request policy and procedure which sets out our approach to subject access requests.

7.19 Individual Rights – Right to Rectification

7.19.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

7.19.2 Where the personal data in question has been disclosed to third parties, Response will inform them of the rectification, where possible. Where appropriate, Response will inform the individual about the third parties that the data has been disclosed to.

7.19.3 Requests for rectification will be responded to within 1 month; this will be extended by 2 months where the request for rectification is complex.

7.19.4 Where no action is being taken in response to a request for rectification, Response will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

7.20 Individual Rights – The Right to Erasure

7.20.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- when the individual withdraws their consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- the personal data was unlawfully processed
- the personal data is required to be erased in order to comply with a legal obligation

- the personal data is processed in relation to the offer of information society services to a child.

7.20.2 Response has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes
- the exercise or defence of legal claims.

7.20.3 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

7.20.4 Where personal data has been made public within an online environment, Response will inform the other organisations who process the personal data to erase links to and copies of the personal data in question.

7.21 Individual Rights – The Right to Restrict Processing

7.21.1 Individuals have the right to block or suppress the processing of personal data by Response.

7.21.2 In the event that processing is restricted, Response will store the personal data, but will not process it further, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. Response will restrict the processing of personal data in the following circumstances:

7.21.3 where an individual has objected to the processing and Response is considering whether there are legitimate grounds to override those of the individual

7.21.4 where processing is unlawful and the individual opposes erasure and requests restriction instead

7.21.5 where Response no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

7.21.6 Where an individual contests the accuracy of the personal data, processing will be restricted until Response has verified the accuracy of the data. If the personal data in question has been disclosed to third parties, Response will inform them about the restriction on the processing of the personal data, unless it is impossible or involves a disproportionate effort to do so. Response will inform individuals when a restriction on processing has been lifted.

7.22 Individual Rights – The Right to Data Portability

7.22.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

7.22.2 to personal data that an individual has provided to a controller

7.22.3 where the processing is based on the individual's consent or for the performance of a contract

7.22.4 when processing is carried out by automated means.

7.22.5 Personal data will be provided in a structured, commonly used and machine-readable form. The information will be provided free of charge. Response is not required to adopt or maintain processing systems that are technically compatible with other organisations.

7.22.6 In the event that the personal data concerns more than one individual, Response will consider whether providing the information would prejudice the rights of any other individual.

7.22.7 Response will respond to any requests for portability within 1 month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by 2 months, ensuring that the individual is informed of the extension and the reasoning behind it within 1 month of receipt of the request.

7.22.8 Where no action is being taken in response to a request, Response will, without delay and at the latest within 1 month, explain to the individual the reason for this and will inform them of their right to complain to the Information Commissioner's Office.

7.23 Privacy by Design and Privacy Impact Assessments (DPIA)

7.23.1 Response will act in accordance with the GDPR by adopting a privacy by design approach, which will seek to ensure that Response have considered and integrated data protection into processing activities where required.

7.23.2 Response has a Data Protection Impact Assessment Policy and Procedure which provides detailed advice on how to undertake DPIAs and when they are used.

7.24 Quality of personal information

7.24.1 For personal information to be of use, it is essential that it is accurate and up to date. Response will ensure the quality of information by.

a) Validating and confirming information with data subjects.
b) Informing data subjects about the importance of providing accurate information.

c) Ensuring that all staff members who obtain and record resident or service user information, record it accurately, legibly, and completely.

d) Giving data subjects the opportunity to check information held about them.

e) Encouraging data subjects to inform Response if any of their details have changed.

f) Introducing monitoring procedures to check the accuracy of data.

g) Incorporating validation processes into new systems.

h) Maintain a high level of quality and timeliness in all data entered onto support, care and housing records.

7.25 Disclosing Personal Data

7.25.1 All personal data will be protected from unauthorised access by appropriate organisational and technical security measures. Personal data will not be disclosed to data processors unless there is a contract or confidentiality agreement in place, which defines the authorised use(s) to which the data can be put. Personal data will not be disclosed to the data subject via a telephone where the authenticity of the requestor cannot be reliably established.

7.25.2 Personal data disclosed to the data subject in response to a Subject Access Request must be reviewed before disclosure to ensure that it does not include any information that infringes the rights and freedoms of any third party or is exempt from disclosure.

7.25.3 Personal data will not be disclosed to third parties where the identity of the third party cannot be reliably established. Personal data will only be disclosed to third parties when one of the following conditions is met:

- the data subject has given Response their consent to disclose the information (including where there is a Lasting Power of Attorney)
- disclosure is essential to the lawful purpose for which the personal data is being processed
- the data subject has given the third party their consent to request the information
- the disclosure is subject to a formal Information Sharing Protocol and is made within the terms of that protocol
- disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)
- disclosure is in the vital interest of the data subject.

7.25.4 Sensitive personal data will only be disclosed to third parties when one of the following conditions is met:

7.25.5 the data subject has given their explicit consent for the disclosure, or a best interest decision has been made – see Mental Capacity Act and DoLS Policy

7.25.6 the data subject has given the third party their explicit consent to request the information

7.25.7 disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)

7.25.8 disclosure is in the vital interest of the data subject.

7.25.9 Disclosure in respect of the last two conditions of this policy must not be made without the formal authorisation of the Data Protection Officer unless delay will lead to serious risk to the data subject or other individual. In this situation the Data Protection Officer will be informed as soon as practicable.

7.25.10 All disclosures of personal data to data processors and third parties will be limited to the minimum information required to satisfy the requirements of the contract or legitimate request.

7.25.11 Consent must be obtained before an individual's personal data is published in any Response publication. In the case of sensitive personal data, the consent must be explicit (e.g., signing of the pre-publication article).

7.25.12 The disclosure of personal data must be recorded in an appropriate IT system.

7.25.13 Access to Information and Disclosure Outside of Response

7.25.14 Members of staff will be granted access to the information that they need to carry out their work. Members of staff have a duty to keep the information they use confidential.

7.25.15 There are a number of occasions where it will be necessary for Response to share PID. The correct parameters of when it is appropriate to share and disclose data include relevant agreements and protocols that are in place that allow for the exchange of information between Response and other organisations. Any information disclosed must be necessary for the purpose for which it is disclosed. Therefore, members of staff should not, for example, disclose details of a member of staff's religious beliefs if only their name and National Insurance number is required by the HMRC.

7.25.16 If it is necessary to discuss individual data subjects in reports or at meetings, a pseudonymisation process should be followed (e.g., Nurse A).

7.26 Client Confidentiality

7.26.1 For further information specifically relating to patient confidentiality, please refer to the Confidentiality Policy and Record Keeping Policy.

7.27 Secondary Uses of Data

7.27.1 A secondary use of data is where PID is used for work not directly related to the care of the client and when information is processed for non-healthcare and medical purposes.

7.27.2 Generally, this could be for research purposes, audits, service management, commissioning, performance management, capacity planning, service redesign and benchmarking, contract monitoring and reporting facilities. {Organisation name} may use data for secondary purposes from time to time but will always ensure that the data is pseudonymised when not being used for direct-care purposes.

7.28 Freedom of Information

7.28.1 Response is only required to provide information under the Freedom of Information Act 2000 in respect of the activities that it carries out whilst under contract with a public authority. As such, Response is not required to respond to FOI requests received directly from members of the public in relation to any other of its commercial activities. The Director of Corporate Governance and Compliance should be advised if a request is made. The Director of Corporate Governance and Compliance will refer the requesting party to the scope of the legislation and politely decline to provide the information.

7.28.2 On receipt of an FOI request that Response must respond to, the Director of Corporate Governance and Compliance will endeavour to ensure that the requested information is collated and returned to the contracting public authority to allow them to meet the 20-working day deadline of the legislation. Prior to sending any information it should be checked for any personal data, which should be redacted prior to sending.

7.28.3 In certain circumstances Response may be asked for our views as to whether certain information should be released before the public body makes a decision as to how to respond. The person responsible for making this decision in Response would be the Director of Corporate Governance and Compliance.

7.28.4 If Response provides any information to a public body on the understanding that it is confidential, this should be highlighted on the documents provided. If information has not been provided to a public body on a confidential basis, the public body may consult with Response as to whether any exemptions under the legislation may apply (for example prejudicing commercial interests).

7.29 Staff Awareness

7.29.1 It is Response's policy that Information Governance training (including data protection and cybersecurity) will be classified as 'mandatory' in the induction programme

7.29.2 all new members of staff to the business will receive information governance training relevant to their role, as soon as possible on commencement of their employment

7.29.3 all individuals associated with Response whether employed or contracted, will receive information governance training at least every 12 months

7.29.4 guidance and support are available to all members of staff who process Personal Data.

7.30 Responsibilities if Response Ceases Trading

7.30.1 If Response is sold to another business, the data relating to our clients will be transferred to the purchasing organisation. Response will notify all its data subjects of the fact that the data is being transferred and that the purchaser will be the data controller from the date of completion of the purchase.

7.30.2 In the event that Response ceases trading altogether, healthcare records will be managed in line with the guidelines contained NHSx Records Management Code of Practice 2021 and retained in accordance with the retention schedule above.

7.30.3 In practice, if the business is liquidated or goes into administration, it is likely that the liquidator or administrator becomes the new most senior member of staff, and they will take over all key decisions.

7.30.4 As a healthcare organisation, Response will still have a legal obligation to continue holding data for a length of time, and as such the business will continue to be the controller of that personal data and data protection laws still apply.

7.30.5 This includes continuing registration with the ICO.

7.31 Information Security

7.31.1 Response has a systematic approach to information security risk management and identifies business needs regarding information security requirements (including contractual and regulatory). During the delivery and maintenance of Response's services, there are a number of instances where risk assessment is necessary (e.g., disclosure to third parties).

7.31.2 The following actions serve as effective risk mitigations when it comes to securing data:

7.31.3 a practical, clear desk policy so that no personal or sensitive information or information of a confidential nature is left on

unattended desks or in offices in such a way that it could be accessible to any person who is not authorised to have such access

7.31.4 information assets and information processing facilities are protected against unauthorised access

7.31.5 information is protected from unauthorised disclosure

7.31.6 confidential and sensitive information is appropriately classified as such

7.31.7 appropriate arrangements are in place to encrypt laptops and emails containing personal information

7.31.8 appropriate arrangements are in place to manage the uploading and downloading of confidential and sensitive information from IT equipment

7.31.9 unsupported systems (including software, hardware and applications) should be identified, and a plan put in place to remove, replace or actively mitigate or manage the risks associated with any unsupported system

7.31.10 confidentiality of information assets is a high priority

7.31.11 integrity of information will be maintained

7.31.12 Response requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities are met

7.31.13 statutory, expressed, and implied legal obligations are met

7.31.14 business continuity plans shall be produced, maintained, and tested.

7.31.15 Access to system, data or networks should be granted only to users that have formally agreed to comply with Response's Information Governance Policy which details how information should be handled and protected. This will be achieved through appropriate clauses in staff and contractor contracts and through the completion of mandatory IG training. Unauthorised and illegal use of information assets and information processing facilities is prohibited. Use of non-Response approved web-applications (such as cloud services) to process confidential information is not permitted without this being approved for use by the Senior Leadership Team. The use of obscene, racist, or otherwise offensive statements shall be dealt with in accordance with other policies published by Response.

7.31.16 This policy is communicated to all individuals working with Response for whom information governance training shall be given. All breaches of information security, actual or suspected, must be reported, and investigated in line with Response policies. Controls are commensurate with the risks faced by Response.

7.32 White Boards

7.32.1 Any PID should not be displayed in an office on a white board where members of the public can view or see from the exterior of the building. Backgrounds should be particularly borne in mind when using video-conferencing facilities.

7.33 Computers

7.33.1 Personal Data must only be stored on Company equipment and not on personally owned laptops or home desktop computers.

7.33.2 IT assets should have a named information asset owner, responsible for the information security of that asset. The Information Asset Register should be maintained by the IT team. All new information systems must be designed to take into account information security and data protection requirements and the management of computers and networks should be controlled through documented procedures. The Information Asset Owner is responsible for ensuring the security of data stored in the named system.

7.33.3 Any changes to information systems, applications or networks should be reviewed and approved in accordance with a documented change management process. Similarly, all information products must be properly licensed and technical controls should ensure that users cannot install software on the organisation's property. Software countermeasures and management procedures must be used to protect against the threat of malicious software.

7.33.4 All files containing personal identifiable information, held on Company owned computer equipment should be "encrypted/password" protected, and preferably not held by the data subject's name, substituting a suitable identifier other than name. Particular care should be taken with portable devices. The ideal is that portable devices should only act as terminals to the main networked system since the data is then protected in the Company network.

7.33.5 Personal identifiable data should not be kept on the hard drives of PCs unless formally justified by the Data Protection Officer, due to the risk of theft and breach of confidentiality. Such data should be stored on the network or authorised applications (e.g. inform), where they will be backed up as required.

7.33.6 Files containing individual person-identifiable information on portable computers should be password protected, or better still not stored on a portable. Files stored on network drives do not require password protecting, as a password is needed to log on to the network and access to folders is restricted.

7.33.7 Users should not leave terminals logged in and unattended. Screens should be locked as soon as the user moves away from the screen to reduce the risk of unauthorised access to information. Computers

should not be transferred between users or disposed of, other than through the IT team as they have the means of transferring or removing all data from the hard drive.

7.33.8 Certain areas within the company have a requirement to have access to information whilst on the move, whether that is by use of a laptop, tablet, handheld computer, mobile phone, or a combination of these. This mobile access creates potential risks to the confidentiality, integrity, and availability of the data we hold on behalf of service users and staff members. This policy sets out how mobile computing is to be used within the company to manage the risk to that data. It also balances the need for easy access to information with our responsibility to the individual to ensure we treat their data properly.

7.33.9 Users of portable computers are to ensure that their device is logged on to the network on a regular basis to receive regular updates to software and anti-virus signature files. If a virus is discovered it should be immediately reported to the IT team and the device and any media used with it, quarantined immediately for inspection and cleaning.

7.33.10 Users issued with a Response owned iPad or iPhone will be connected to their email and calendar functions by use of the Company's selected Mobile Device Management (MDM) software solution. The MDM software ensures security of the company data, and, that there is no interaction between the company data and the remainder of the device.

7.33.11 Users are forbidden from attempting to 'jailbreak' the device or otherwise attempt to alter its security configuration. Users are also forbidden from downloading and installing applications without prior approval from IT.

7.33.12 Response and its IT Team shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All clients shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the IT team. Users breaching this requirement may be subject to disciplinary action.

7.33.13 As working practices change and staff members become more mobile there is now a need for users to access their email, calendar and working documents from outside of the normal office environment.

7.33.14 Where there is a requirement for a user to work away from company premises, remote connectivity is only to be used via the company Virtual Private Network (VPN). Use of the company VPN system requires that users are issued with the relevant software and login credentials.

7.33.15 It is a user's responsibility to ensure that their credentials are kept safely and securely. Credentials must be kept confidential and not

disclosed to anyone. Secure VPN Access can be requested from the IT Team.

7.34 Telephones

7.34.1 All possible steps must be taken to ensure that information regarding an individual is not divulged over the telephone to anyone without authority. Asking for key details about the individual (e.g., date of birth) may not be sufficient to ensure that the caller has a need to know.

7.34.2 Where there is any doubt regarding the identity of the person requesting the information, guidance should be sought from the Data Protection Officer. If advice is not immediately available, then the information should not be disclosed. If the caller is claiming to be from an organisation (e.g., the NMC) then the switchboard telephone number should be obtained (rather than direct line), checked and then used to ensure that the caller is from the agency stated.

7.34.3 A record should be kept of all telephone discussions where information is shared verbally on the personnel file.

7.35 Email

7.35.1 Personal email addresses should never be used for work purposes. Person identifiable information must only be sent by e-mail within Response when attached to a password protected document, spreadsheet, or database. Inclusion within the main body of the e-mail is not permitted. The password should be delivered to the intended recipient by a different medium, such as a telephone call or text message.

7.35.2 Personal identifiable information must only be sent externally using an encrypted email. Steps must be taken to ensure that any confidential/sensitive information is sent to the mailbox of the person or persons who are authorised to see that information, and that no unauthorised persons have access to that mailbox/those mailboxes.

7.35.3 Before sending or receiving confidential/sensitive emails, confirm the email address with the other party, spelling any words that may cause errors. Use must be made of the e-mail “Tracking Options” where available, to notify that a message has been delivered and/or read. Otherwise, the sender must be telephoned to confirm receipt. A copy of the e-mail and its attached documents must be stored appropriately within manual and/or electronic records, and the original email deleted from both the inbox and deleted items.

7.35.4 All members of staff should be mindful of using the ‘reply all’ and ‘cc’ buttons to prevent against other people receiving information unnecessarily. There must be a justified reason for anyone to be copied into or sent PID.

7.36 Video Conferencing

7.36.1 Prior to utilising any video conferencing (or otherwise) software a Data Protection Impact Assessment should be carried out to determine the implications of using the new technology on the privacy rights of individuals.

7.36.2 Privacy settings of all software should be examined thoroughly to determine their adequacy. The rights of data subjects should also be kept in mind to when choosing a software service (e.g., the ease in which chat data can be extracted which may relate to an individual).

7.36.3 Members of staff should also be mindful of their backgrounds when using video conferencing facilities and ensure that no identifiable information is visible behind them.

7.36.4 It is also important to be aware that there may be other people within the room that cannot be seen on screen or are within earshot and as such confidential or private information should not be disclosed as a matter of course, without first checking with the individual whether they agree to this.

7.36.5 Video conference chats should not normally be recorded without obtaining the consent of the individual involved and if this is done, the privacy notice should be updated to reflect this.

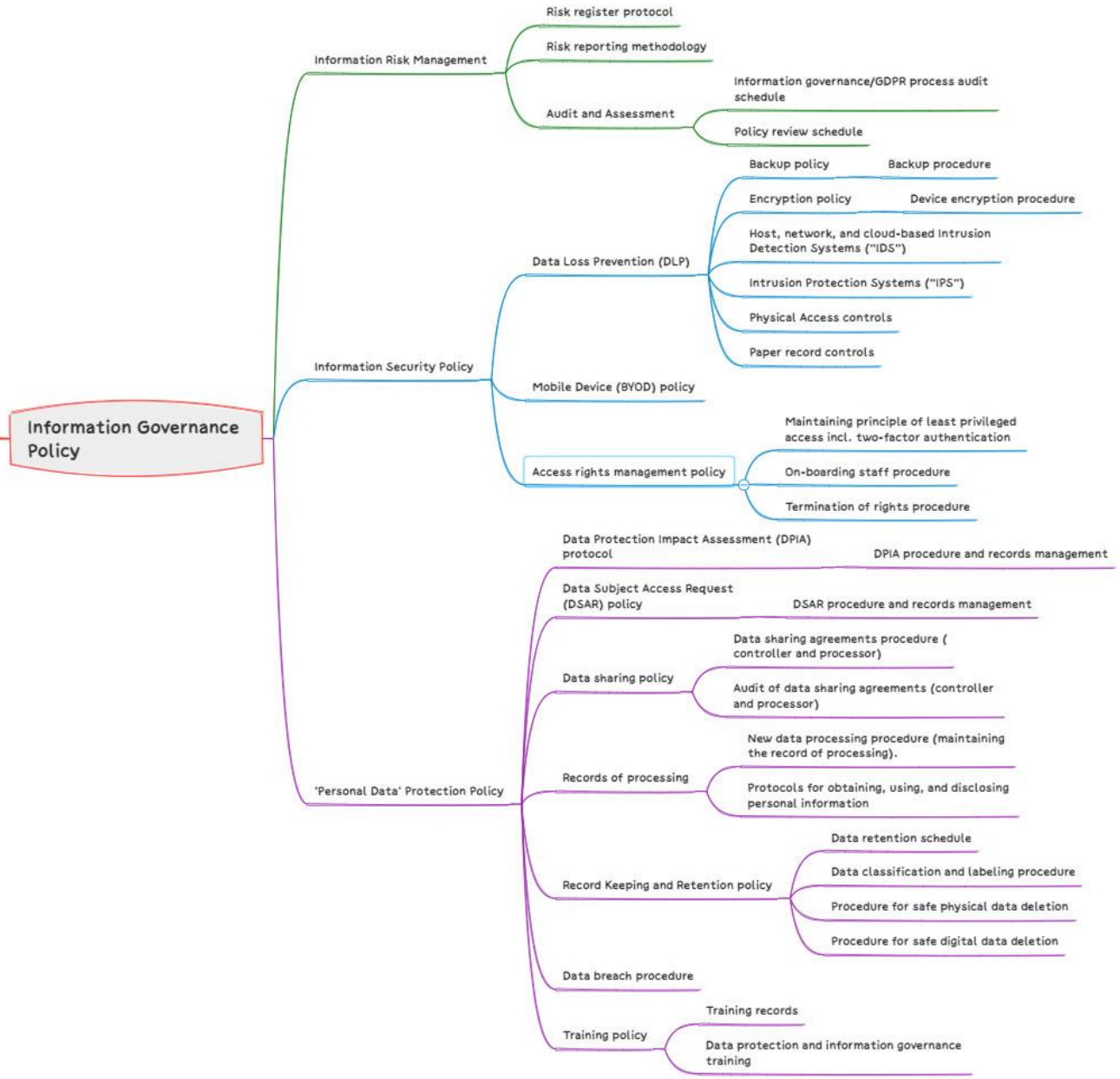
8. RELATED DOCUMENTATION

The following policies, protocols and procedures are referenced in, or refer to, the Data Protection Policy.

9. Appendix 1: Diagram of related policy and procedures.

Response
Together we can achieve change

Corporate Governance Policy



3.0

10. Appendix 2 Table of related policy and procedure

Document name	Location
Information Governance Policy	
Information Security Policy	
Data Subject Access Request (DSAR) policy	
Data sharing policy	
Record keeping and data retention policy	
Training policy	
Records of Processing Activities (ROPA)	
Data Protection Impact Assessment (DPIA) protocol	