TAC Healthcare

Information Governance and Security Policy

Document Number	TAC/ISMS/PD/6026	**Version**	2	**Pages**	Page **1** of **41**
Date of Last Review	22 June 2023	**Date of Next Review**		June 2025	
Approved by **Print Name**	Signature [redacted] Wendy Sharp, Quality & Compliance Manager				
Executive Sign-Off **Print Name**	Signature [redacted] Ken Park, Clinical Director				

Document control – revision history

Date amended	Version	Revision	Approved by & date
08/10/18	1	Audited and updated to include document number, new logo and footnote table – W. Sharp	A. Duncan 08/10/18
02/02/22	1.1	Reviewed and updated to reflect TAC changes	W. Sharp 02/02/22
4/11/22	1.2	TAC logo updated and link to Data Breach Policy inserted	W Sharp 4/11/22
22/06/23	2	Updated to incorporate aspects of InHealth IG Handbook	W Sharp 22/06/23

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Contents

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in Clinical Governance, service planning and performance management.

It is of paramount importance to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability structures are in place to provide a robust Information Governance and Security (IG&S) framework for information management.
TAC Healthcare Ltd (TAC) holds and manages a great deal of personal and confidential data relating to patients, employees and clients, including commercially sensitive information. With consistent changes to both technology and demands supporting ever-easier ways by which information can be accessed and shared it is important that a consistent approach is adopted to safeguard all parties.

This policy sits within our Information Security Management System (ISMS) and details the arrangements in place to provide a robust framework in TAC to ensure personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.
This policy is designed to set the standards expected in order to maintain the security of information within our organisation. Its implementation will ensure a safe and secure environment for information held both manually and electronically. In particular, that this information is operated in accordance with Information Security, Information Governance principles, Caldicott Guardian Principles and relevant legislation. The policy has been developed in line with NHS Data Security Toolkit, ISO 9001 – Quality Management, ISO 27001 - Information Security.

This Information Governance & Security Policy also aims to embed the concept of identifying, recording, managing and protecting Information Assets (IA) and associated risks within the wider risk management framework. It is intended to:

- Ensure identification and safeguarding of all vital information assets
- Link to the wider organisational risk management framework, in which information risks will be identified, considered and addressed in key approval, review and control processes
- Meet contractual and legal requirements
- Meet standards set through internal and external assessment obligations

TAC has put this policy in place to ensure its staff (including those directly employed or working on behalf of the TAC) are fully aware of information governance and security and their responsibilities.

All information must be handled effectively and efficiently within the context of:

- **Confidentiality:**
  Protecting information from unauthorised disclosure

- **Integrity:**
  Safeguarding the accuracy and completeness of the information

- **Availability:**
  Ensuring that information and vital services are available when required.

This policy is important as it should help staff to understand how to maintain the integrity and security of the information effectively and consistently, we hold, in line with current UK legislation.

As information is a valuable asset that helps us to effectively make informed decisions, it is important that we make sure its security and protection are adequate and effective across our business. To do this we will ensure information is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically, and
- Shared and disclosed appropriately and lawfully.

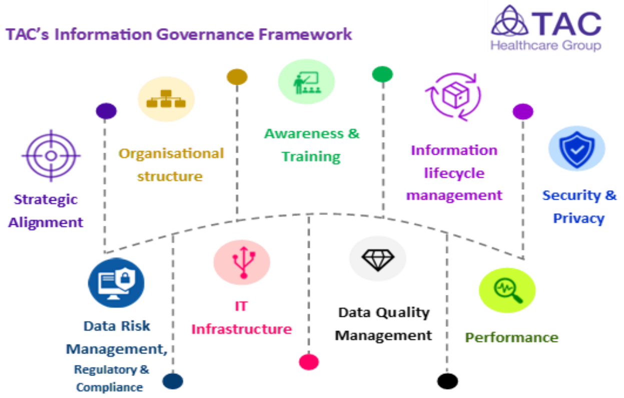
TAC is committed to ensuring that information in whatever its context, is processed as determined by prevailing legislation, statute and best practice. Compliance with all organisation policies is a condition of employment and a breach of policy may result in disciplinary action. In addition, breach of this policy may be considered as a breach of the Computer Misuse Act and treated as a criminal offence.

2. Scope

TAC Healthcare (TAC) holds information in many forms such as electronic records, paper files, patient records, staff records, contracts videos, images all known as Information Assets (IA).
It is important that these IA are protected for the following reasons:

- Assure our patients, staff, clients, and other stakeholders that their information is secure.
- Satisfy legal requirements and avoid monetary penalties.
- Avoid reputational damage.

The purpose of this document is to describe the policies and approach that create our framework to manage, store and protect all IA. This document must be read in conjunction with the Computer and Mobile Phone Acceptable Use Policy, Data Protection Policy, Information Asset Management Process, Data Retention and Disposal Policy, Information & Risk Assessment & Management Policy, Whistle Blowing Policy and Medical Records Policy.



Information Governance (IG) is formed by those elements of law and policy from which applicable IG standards are derived. It encompasses legal requirements, central guidance and best practice in information handling including:

- The common law duty of confidentiality
- Data Protection Act 2018
- Human Rights Act
- Information Security
- Information Quality

- Records Management
- Freedom of Information Act 2000

Information Security (IS) are the measures and protections in place to protect all IA when establishing, implementing, holding, obtaining, recording, using, sharing and disclosing of data/information or records held by TAC in a manual/paper or electronic format.

This policy applies to but is not limited to; staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other representative of the TAC such as contractors, students or visitors; any holding companies; business partners.

TAC has two distinct settings where its Information Security are key:

- **Internal** – this is our integrated management system and is maintained by our IT support team which sits within Quality & Compliance.
- **External** – this is made up of three aspects; IT support to assist with more technical enquiries, bespoke cloud-based support systems and licensed software systems.

3. Purpose

The purpose of the policy is to provide a policy statement on the use, management, storage and protection of information held by TAC and describe the arrangements for providing assurance to TAC Board that IG and security standards are defined and met, and any breaches are managed appropriately.

The Policy is intended to achieve and maintain the following Information Governance and Security objectives:

Confidentiality	Assuring that confidential information and systems are accessible to only authorised individuals through appropriate and lawful mechanisms and is not disclosed/available to unauthorised individuals or the public.
Integrity	Safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.
Availability	Ensuring that information, systems, networks and applications, as well as paper records, are available when required to departments, groups or users that have a valid reason and authority to access them.
Accountability	Users will be aware of their responsibilities in relation to their collection, use and processing of data and information.

4. Terms and Definitions

Throughout this policy the following terms will have the agreed definitions:

Term	Definition	Source
Data	Data is used to describe ‘qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)1 based on the Cabinet

Information	Information is the ‘output of some process that summarises interprets or otherwise represents data to convey meaning.’	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review ‘personal’ includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and ‘confidential’ includes both information ‘given in confidence’ and ‘that which is owed a duty of confidence’ and is adapted to include ‘sensitive’ as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
IGSoC	NHS Digital Information Governance Statement of Compliance The Information Governance Statement of Compliance (IGSoC) is the process by which organisations enter into an agreement with HSCIC for access to the health and Social Care Network (HSCN). The process includes elements that set out terms and conditions for use of HSCIC systems and services including the HSCN, in order to preserve the integrity of those systems and services. The steps in the IGSoC process set out a range of security related requirements which must be satisfied in order for an organisation to be able to provide assurances in respect of safeguarding the N3 network and information assets that may be accessed.	
DSP	The Data Security and Protection (DSP) Toolkit is an online tool that TAC must complete annually to evidence compliance with the data security and information governance requirements. The Department of Health and Social Care (DHSC) has mandated that all organisations with access to NHS patient data and systems must use this Toolkit to carry out self- assessments.	Data Security and Protection Toolkit (dsptoolkit.nhs.uk)
ISO27001:2013	An international standard that helps manage the security of assets such as patient information, intellectual property, employee details or financial information.	

ISMS	A key element of the ISO27001, an Information security management system is a systematic approach to managing confidential company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.	

5. Principles

- There should be proactive use of information within the organisation, both for patient care and service management as determined by law, statute and best practice.
- There should be proactive use of information between TAC and other partner organisations to support patient care as determined by law, statute and best practice.
- TAC will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Data Security & Protection Toolkit.
- TAC will follow a program of continual improvement to increase IG&S compliance year on year.
- All staff must complete annual GDPR and Data Protection training and are expected to maintain their knowledge by attending additional awareness sessions to equip them to meet their individual responsibilities in relation to IG.
- Where appropriate the principles of information management and handling outlined in this policy are to be applied to all identifiable documents.
- All new developments and changes to policies and procedures will require a Data Protection Impact Assessment (DPIA) assessed to identify any impact of information handling and information quality.

To adhere to these principles TAC has committed to:

User education and awareness	TAC produces user security policies that describe acceptable and secure use of our ICT systems and are formally signed off by the individual. ISMS is included in all induction training and is included in our annual mandatory training programme.
Incident management	It is the intention to introduce annual testing of our disaster recovery and business continuity plans. TAC will report online crimes to the relevant law enforcement agency as necessary. All incidents are reported via our incident reporting process and investigated.
Malware prevention	TAC has in place policies that directly address the business processes (such as email, web browsing, removable media and personally owned devices) that are vulnerable to malware. Malware is scanned for across the business.
Monitoring	All incidents are reported and monitored by Incident & Risk Group that reports in to the IRMG. This themes incidents and takes account of previous security incidents and attacks, and TAC's incident management policies.

	There is continuous monitoring of inbound and outbound traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. All user activity is restricted, particularly all access to sensitive information and privileged account actions (such as creating new user accounts, changes to user passwords and deletion of accounts and audit logs) is extremely limited.
Control Removable Media	Where the use of removable media is unavoidable, limit the types of media that can be used together with the users, systems, and types of information that can be transferred.
Manage Remote Working	Assess the risks to all types of mobile working (including remote working where the device connects to the corporate network infrastructure) and develop appropriate security policies. Train mobile users on the secure use of their mobile devices for locations they will be working from. Apply the secure baseline build to all types of mobile device used. Work towards creating our Domain to protect data-at-rest and data-in-transit.

All of these are covered within this policy or corresponding policies and procedures published in TAC's Quality Management System. Readers should ensure that they are aware of these and are read in conjunction to this policy.

6. Roles and Responsibilities

Information Governance and Security is everybody's business and therefore it is everybody's responsibility to ensure information is secure for all interested parties. This section describes the expected responsibilities in relation to Information Security of persons processing information.
It is noted that some individuals will hold more than one role.

Role	Responsibilities
Governing Body	The Governing Body will ensure that its organisation has taken appropriate steps to meet IG standards. In particular it will seek assurance against Information Security compliance. The Governing Body delegate the approval and monitoring of compliance to the Quality & Compliance (Q&C) Team.
Caldicott Guardian	The Caldicott Guardian is an advisory role appointed by the Governing Body acting as the conscience of the organisation for management of personal information and a focal point for confidentiality and information sharing issues. The Caldicott Guardian is supported in this role by the IG Manager and other key staff both internally and externally where appropriate. The duties and responsibilities of TAC Caldicott Guardian are outlined in Caldicott Principles Policy.

Clinical Governance Committee (CGC)	The CGC are delegated to monitor and manage all aspects of this policy, escalating where appropriate any issues or concerns. The CGC has overall accountability and responsibility for governance and will provide assurance that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
Incident & Risk Management Group	The IRMG will review and analyse all risks to identify trends for reporting to the Clinical Committee Group
Senior Information Risk Owner (SIRO)	The SIRO is the appointed officer responsible for overall information risk management within TAC. This role has overall responsibility and accountability for ensuring that effective systems and processes are in place to address the Information Governance agenda and in particular Information Security principles. The SIRO is supported by CGC and IRMG & Caldicott Guardian in fulfilling this function in relation to Information Security.
Directors (Information Asset Owners)	All Directors are required to act as Information Asset Owners (IAO) for the information assets within their remit. They will provide relevant assurance to the SIRO that information risk is managed effectively for the information assists identified as within their remit. The Q&C Team will support IAO's to ensure that nominated Information Asset administrators are identified and are taking necessary actions to comply with this policy.
Senior Managers (Information Asset Administrators)	Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how they work and how they are used. They will ensure there are procedures for using specific information assets, manage and control access (add and delete) to them and understand their limitations.
Managers	All staff with a management or supervisory role have a responsibility to ensure that all staff and employees working in their respective areas have been provided with adequate corporate and local guidance on information security for potential issues within their area. Managers can seek support in fulfilling this role from the CEO/CD.
Super Users	Super users have slightly more admin rights and are appointed by each department to: •Edit and upload •Create unique views and assigned to libraries and lists where approved •Advise department on SharePoint •Draft news posts for management approval
All Substantive/ Permanent Staff	All staff and those working for TAC have a duty outlined in their terms and conditions of working with (or on behalf of) TAC to adhere to the principles outlined in this policy. Any member of staff that acts outside of this policy may be liable to disciplinary action which can lead to dismissal or criminal charges under the Computer Misuse Act.

Contractors/Temps /Agency	The same responsibilities as for permanent staff apply to those working on behalf of TAC organisation, whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of but not directly employed by TAC are required to sign a third-party agreement outlining their duties and obligations. This is normally covered when they register with an approved agency or as part of their documents issued by HR.
TAC Member/ Partner Practices	This policy should be followed where any member or partner is processing information on behalf of or in relation to TAC.
IT System and Service providers	Third Party organisations and system providers will provide secure, reliable IT network infrastructure with associated controls for information and cyber security. Local controls will be validated as part of the commissioning process, and assurance will be provided to Q&C.

TAC CGC has been delegated powers from on behalf of the Board to oversee and monitor IG&S in TAC. The Board will seek the necessary assurance that TAC is achieving the required compliance with IG requirements outlined in the DSPT. IG will be a standing agenda item at CGC and Incident & Risk Management Group (IRG) meetings and a report on IG will be submitted to the Board annually.

The primary responsibilities of TAC CGC and IRMG Group are:

- To monitor IG&S policy and procedure and ensure any changes to legislation or national policy are reflected in local IG policy and procedure.
- To complete and submit the assessment of compliance with IG requirements published in the DSPT and provide assurance that the minimum mandated level of compliance is met.
- To develop and implement a programme of improvement designed to show year on year improvement in IG compliance across TAC as measured by the DSPT assessment.

7. Quick overview - Do's and Don'ts

TOPIC	Do	Don't
Passwords	Change every 6 months	Share with anyone
USB stick	Only use one provided/approved by TAC	Use your own memory stick
TAC equipment	Use it for work purposes only	Download music, games or videos
Copyright	Check you can use the information you copy before you paste.	Assume it is freely available - see Copyright law
Away from your desk	Lock your screen and clear your desk	Leave your monitor on so people can see what you are working on.
Training	Complete annual Data Protection mandatory training	Wait for your manager to chase you
Data Breach	Report any concerns using the Incident Reporting process	Panic and keep quiet!
Leavers	Report this to IT so access rights can be removed	Forget to get equipment back

For more guidance please see Appendix E

8. Information Assets & Register

Information as with any other assets of the organisation should be seen and recorded as an asset, which can take many forms. For the purpose of this policy the key assets that Information Asset Owners (IAOs) should be identifying are within Appendix C.

Information Assets (IA) are those that are central to the efficient running of departments within the Council, for example, service user information, social care information, card holder data, health information, commercial documents, finance information, staff files etc.

Physical assets include the computer systems, network hardware and software, which are used to store and process this data. It also includes physical assets, such as, infrastructure, equipment and accommodation used for data processing.

The Information Asset Register (IAR) must be used to record all information assets and the Asset & Calibration Register to record physical assets.

Manual and electronic information managed by Information Asset Administrators (IAAs) and IAOs fall under the categories:

- Records containing personal information such as HR and Patient files and electronic systems with the data within records
- Corporate records such as policies procedures, minutes, decisions on service delivery, etc.

Once information assets have been identified, the IAOs must ensure that they have been logged on the Information Asset Register along with the risks and corresponding controls.
IAOs must ensure that information assets are assessed for risk regularly in line with Risk Management Policy and guidance. Results of risk assessments should be placed on risk registers and escalated as per the Risk Management Policy and guidance.

Where suitable controls are not in place, an action plan is to be agreed with the relevant IAO, IAA and Q&C Team on behalf of the CGC and IRMG to address any shortfalls and risks recorded on the corporate risk register.

9. Legal ownership of information and data

TAC has legal ownership of the contents of all business files stored on its computer and network systems, except in relation to data being processed by TAC as data processor, as well as all business messages transmitted via these systems. TAC reserves the right to access this information without prior notice whenever there is a genuine business need.

10. DPIA

Article 35(1) of the GDPR says that you must do a DPIA where a type of processing is **likely to result in a high risk** to the rights and freedoms of individuals.

The ICO states that 'A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.'

Please complete the Data Protection Impact Assessment.pdf for any type of data processing that has been assessed as high risk and submit it DPO@tachealthcare.com for consideration by the DPIA Review Panel.

11. Integrated Quality Management System

It is the policy of the TAC that all work-related activity must be conducted through our SharePoint Integrated Management System. This not only protects the business from loss of data but mitigates the risk when key people have unplanned absences.

Shared network resources should be backed-up daily for recovery of failed equipment and removed to an offsite secure storage facility weekly for recovery of a denial of access business continuity event.

All stored data has defined clear owners.

Retention periods for data must conform to local business requirements, and with statutory and regulatory requirements. TAC Management must conduct regular reviews to ensure compliance with these requirements. Personal data must be retained, processed and transferred only in accordance with personal data legislation.

11.1 Using SharePoint effectively

TAC's bespoke central repository, (TAC Healthcare - Home (sharepoint.com)) is accessible to all TAC staff who are registered with appropriate access and permissions designated by their line manager.

This SharePoint repository allows staff to collaborate on working documents with access to document libraries, lists and managements systems created and owned by TAC. Examples of these systems are:

- TAC Quality Management System
- Continual Improvement Register
- Information and Asset Register

As SharePoint is part of the Microsoft 365 suite of applications specific libraries and lists can be synchronised to allow users to access via file explorer for document upload, etc.

Users are encouraged to use OneDrive for their own working documents which again can be synchronised as part of the Microsoft 365 application.

12. General IT Security Standards

This policy is part of a suite of policies and procedures supporting TAC's Information Security Management System and Governance responsibilities.

The following sections set out the standards that those working for or on behalf of TAC are expected to adhere to when in relation to Information Security.

12.1 Information Risk Management

Cyber security is a threat to the security of both information and operations of any organisation.

TAC has implemented the following 10 stage approach (developed by the GCHQ) to support the mitigation of risks arising from this.

Information Risk Management Regime	Assess the risks to TAC information assets with the same vigour as they would for legal, regulatory, financial, or operational risk. Embed an Information Risk Management Regime across TAC, supported by the Board and senior managers. Communicating our risk management policy across TAC so all employees, contractors and suppliers are aware of our risk management boundaries.
Secure Configuration	Use of formal processes to manage the configuration and use of our ICT systems. Removal of unnecessary functionality from ICT systems and keeping them patched against known vulnerabilities.
Network Security	TAC filters and monitors all traffic at the network perimeter so that only traffic required to support the business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).
Managing User Privileges	All users of our ICT systems are only provided with the user privileges that they need to do their job. TAC controls the number of privileged accounts for roles such as system or database administrators and ensure this type of account is not used for high risk or day-to-day user activities and is included in a specialist agreement sign-off.
Education and Awareness	This policy should be formally acknowledged and signed off as ‘read’ by all staff.
Incident Management	All IG&S incidents will be reviewed and managed by CGC and IRMG with specialist oversight as required.
Malware prevention	IT will ensure that anti malware and anti-virus protection is up to date and actively scans all machines and systems
Monitoring	IT will audit use Computers, mobiles and email to ensure the Computer & Mobile Phone Acceptable Use Policy is adhered to

12.2 Accountability and Governance

TAC has put in place suitable controls to:

- Assign responsibilities to oversee the delivery of standards set out in this policy
- Report on compliance against relevant standards to the CGC.
- Ensure that all staff are aware of their responsibilities, how to comply with them and have available advice and guidance and training to do so.
- Support and develop relevant security policies and procedures for local systems and services as necessary.
- Ensure compliance with Data Protection, and other information security related legislation.

12.3 NHS Data Security & Protection Toolkit Assessment (DSPT) Procedure

TAC will annually complete a self-assessment of compliance with the requirements applicable to TAC in the current version of the NHS Data Security & Protection Toolkit Assessment (DSPT). The summarised results of this assessment are the made public on the DSPT and details are shared with regulators such as HIS & CQC to assist with their continual assessment.

All assessments are completed by making a formal declaration of the level of compliance assessed for each requirement and identifying and uploading copies of appropriate evidence (documents, policies, meeting minutes etc) to support the level of compliance assessed.

Each requirement in the DSPT will be allocated to an IG&S initiative led to manage and assess. The appropriate lead will be responsible for assessing compliance in line with the guidance and criteria set for the requirement and maintaining the currency of the evidence supporting the declared assessment level.

Prior to each assessment submission the CGC and IRMG will review and approve the proposed assessment and, where necessary, action any improvements to ensure compliance.

Following approval, a report will be submitted to the Board summarising the proposed assessment and seeking approval for the submission.

13. Change Management

The introduction of change can have an adverse impact on the quality, security and confidentiality of the information we handle. A Management of Change Form must be completed and should consider the need to conduct a full Data Protection Impact Assessment.pdf to assess the impact on IG&S resulting from a change.

Guidance for staff in how to undertake an assessment of the impact of proposed changes on IG&S standards and processes is included at Appendix C.

14. Managing Security and Information Risk Assessment

TAC is working towards ensuring all staff are able to identify and manage information risks in line with existing risk management policy and processes.

A failure to effectively implement information could lead to the following risks:

Risk	Example
Reputational	Making decisions from inaccurate information could undermine any commissioning decision and could affect organisational reputation.
Financial	Loss of information could lead to financial penalties of up to £500,000. Inefficient use of information may lead to duplication and wasted time.
Failure to comply with legal, or regulatory	There are a number of lawful requirements to manage information such as the Data Protection Act, Public Records Act which could also lead to reputation or financial loss.

15. IG&S Incident management

All staff are responsible for ensuring that any actual or potential Incident is reported using our Incident Reporting Form in line with the TAC Accident, Incident, Adverse Incident and Near Misses Policy which covers Information Security related incidents.

Such incidents include, but are not limited to:

- Loss or potential loss of Personal Data/Information
  - Lost Records
  - Stolen files, diaries, Memory Sticks, Laptops, CDs etc
  - Theft of IT equipment
- Breach of Confidentiality
  - Unauthorised disclosure of information e.g. release of confidential information to the wrong person, people opening the wrong mail, faxes sent to the wrong place/person, post not arriving to its intended destination
  - Leaving confidential/sensitive files out
- Inappropriate use/access to personal information
  - Access to data/information is not restricted
  - Personal Data/Information left unattended
  - Using/sharing another user’s login id and password
  - Accessing a person’s record inappropriately e.g., viewing records of family members, neighbours, or friend etc.
- Technical Incidents
  - Hacking
  - Hardware faults
  - Internet misuse
  - Malicious damage, including misuse or malicious software
  - Computer virus, worms and Trojans
- Other Incidents
  - Natural disasters
  - Physical security
  - Suspicious activity
  - Theft/Loss

All breaches of physical security (building security) must also be immediately reported to the HSSE and Facilities Manager.

Incident Investigation

Any incident investigation will take place in line with guidance, with any incident identified as a serious incident following a root cause analysis approach. All serious incidents will be formally reported to the CGC for review and monitoring of actions to reduce impact and prevent repeated incidents.

Forensic Examination

Forensic Examination is the ability of an organisation to make use of evidence when required. Any investigation involving Information and Communications Technology (ICT) systems is likely to involve digital evidence and may therefore involve forensic examination.

Forensic Examination may be used when necessary, as part of an incident investigation process. To ensure evidence is not corrupted specific procedures will be put in place to protect the validity of electronic evidence. Please speak with IT should this be required.

16. Continual Improvement

TAC IG&S strategy is to follow a programme of continual improvement to show a year-on-year increase in IG&S compliance as measured by the annual assessment against the IG&S requirements set out in the DSPT.

The results of the previous DSPT assessment will identify key areas for improvement and will be used in conjunction with audit findings and other sources of information to identify priorities for action.

Any areas for improvement will be added to the Improvement Plan and reviewed at the monthly IRMG for reporting up to the CGC.

17. Data Breaches

All staff should ensure they are familiar with the Data Breach Policy.pdf and how to manage and report **all** suspected or confirmed data breaches immediately via the Incident Reporting Form.

Internal and External Reporting of Incidents and Risk

TAC must report those Information and Cyber Security Incidents that are deemed to be an IG&S **Serious Incident** Requiring Investigation (SIRI).

The IG&S incident scoring is determined by the context, scale and sensitivity based on NHS guidance.

Every incident can be categorised as either:

1. Confirmed IG SIRI but no need to report to ICO, DHSC and other central bodies.
2. Confirmed IG SIRI that must be reported to ICO, DHSC and other central bodies.

18. Removeable Media

As TAC's Quality Management System is in SharePoint there should be little to no need for removable media such as USB memory sticks. However, if required these must be provided and/or approved by TAC It prior to use.

18.1 Copying Files to USB- Attached Storage Devices

Only files relating to the relevant work of employees can be copied, subject to item 17.

Relevant files would include files in their own file space which they have produced and files in another's file space to which they have been granted permission to copy.

18.2 Computer operating systems

Files' belonging to a computer's operating system and its installed applications must not be copied.

18.3 Confidential data

Where confidential data (clear direction is given on information classification in Document Classification & Control Policy) has to be stored on removable media then such media must be encrypted unless written authorisation by senior management is obtained for specific exceptions.

Encrypted USB memory sticks must be requested from IT and have a reasonable business case.

18.4 Copying File from USB- Attached Storage Devices

Only files relating to TAC's work can be copied, subject to Section 1. This includes copying files to their own file space and copying files to another's file space to which they have been granted permission to copy.

Files which may be detrimental to the performance and/or stability of either the computer being used, or another network-attached computer must not be copied to the computer being used.

18.5 Execution of Files Stored on USB – Attached Storage Devices

It is not permitted to execute program files or script files that are stored on the storage device, except where expressly told to do so by the IT department. The file may have an adverse effect on the performance or stability of the computer on which it is executed.

18.6 Suitable Devices

Devices deemed as suitable for attachment to the USB ports of TAC computers and laptops have one thing in common: they do not require device driver software to be installed and must be capable of operating under the built in drivers of the computers' operating system.

If an employee wishes to attach another type of USB device, they should contact the IT Service Desk in the first instance**.**

19. Copyright and Data Protection

As an employee of TAC, you should be aware of the requirements of the Caldicott Guidelines and IGSoC, including the Data Protection Act, which relates to privacy of personal information, and any related guidance.

- Employees must comply with the provisions of the Copyright, Designs and Patents Act 1988.
- Employees must comply with the provisions of the Data Protection Act 1998.

20. Data/Information Classification

All information assets should be classified and marked according to the following terms:

Marking	Description
Unrestricted	Non classified – available for open use and can be shared outside of TAC.
Confidential	Data that is covered by the DPA or relevant legislation as Personal Identifiable information e.g. patient clinical records
Commercially Sensitive	Data that has a commercial value (limited) e.g. commercial contracts

21. Recruitment and Contracts of Employment

TAC has in place

- Recruitment and selection processes that ensure
  - Proof of identity to PVG level 3 standards
  - Reliability to work within the organisation and with relevant sensitive data
  - Contracts of employment which contain appropriate clauses to maintain the confidentiality, availability and integrity of data in line with this and relevant policies.

- Staff Changes processes (Starters Leavers and Movers)
  - Managers are responsible for notification of new staff or changes in role which affect access rights to any IT Systems
  - Managers retain responsibility to ensure access rights are appropriately established from effective dates.

22. Business Continuity and Disaster Recovery

All systems used by TAC are cloud hosted and backed up on a daily basis including our SharePoint system. Individual devices are also backed up on a daily basis.

This allows for all systems to be resumed as soon as is physically possible should it be required.

As outlined in the Business Continuity Plan, all critical systems, applications and data can be accessed on alternative hardware.

23. PCs and laptops

Only devices provided by IT and therefore encrypted should be used to access TAC systems and files unless in an emergency or with given clear and specific permission from IT and with sign off from the user's line manager. If this is allowed, then IT will perform checks prior to the start of the access on the device that is to be used to ensure that the equipment is safe and adequate.

24. Electronic Information Security

Networks

TAC recognises the need for a secure and reliable system to transfer electronic information securely and efficiently as a critical system to enable the delivery of business. TAC IT support will make provisions to ensure the network is secure in line with the requirements set out within this policy, supporting guidance and industry best practice.

Remote/Off Site Access

Any access to Information remotely or off site must be secure and handled as it would on site in line with this policy. TAC, at its discretion, will provide staff with access to computer networks and systems in line with this policy and underpinning guidance and procedures.

Any equipment provided will remain the property of TAC and items such as Laptops, mobile phones and any other equipment provided by TAC should only be used by the allocated member of staff for business purposes other than pre-approved personal use.

25. Wireless Communication

This policy prohibits access to TAC and its IT Service provider networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy are approved for connectivity to these networks.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of our internal networks. This includes any form of wireless communication device capable of transmitting packet data.

A risk assessment must be undertaken before any Access Points are implemented. This ensures the scope of the security measures will be adequate for the risks associated with the network.

Under no circumstances should you connect any TAC device to an unsecure external wireless network including public locations such as Cafes and restaurants, connecting to an unsecure network leaves your device open to hackers and viruses. To do so will be regarded as Gross Misconduct and may be subject to instant dismissal.

If you are in one of these locations and require an internet connection for your TAC device, please use your TAC mobile hotspot or wait until you are in a location with a secure suitable network.

26. Use and Installation of Software

Any use of software must have been approved by the TAC IT department as being suitable for use and installation.

Approval will be based upon:

- Review of licensing compliance with proposed use
- Ensuring compatibility with currently installed systems
- Arrangements for support and updates

Software installation should be by TAC IT department or the relevant IT service provider following the suitable checks. Staff should note that it is a criminal offence to make/use-unauthorised copies of commercial software and offenders are liable to prosecution.

27. Acceptable use of IT Systems

All IT systems, software and hardware provided by TAC to its staff and other users is for direct business use only. Any personal use of IT systems and services is strictly restricted by TAC and the IT department.

Any approved use must ensure that personal use:

- Does not interfere with the performance of your duties
- Does not take priority over your work responsibilities
- Does not cause unwarranted expense or liability to be incurred by the organisation
- Does not have a negative impact on the organisation in any way
- Is lawful and complies with this policy
- Not be accessed in areas that are in view of patients or members of the public

The following items are not an exhaustive list but must not be stored for personal use in any location on company devices:

- Music Files
- Video/Films Files
- Games/ Other unauthorised Software
- Inappropriate images (including any of children or minors including family members).

Staff using this facility accept that any document/file held on TAC provided equipment or systems are subject to review and access by Q&C and the TAC IT department as part of the internal auditory functions.

If after investigation, any files/documents or images are found they will be removed automatically prior to any notification. Any repeated misuse will be deemed as breach of this policy and subject to disciplinary and/or legal action.

This does not apply for authorised business-related use (authorised by a line manager), however the items will need to be stored in alternative network storage to a given personal drive.

27.1 Internet Access

TAC provides access to the internet and its resources for the purpose of conducting Company business and not any other business. Incidental personal use is permitted, provided it does not interfere with the individual's business responsibilities or the operation of the Company's Internet gateway, and provided it complies with all the rules set out in Electronic Communication and Social Media policy.

27.2 Email

The Company provides e-mail capabilities to individuals for the purpose of conducting Company business and not any other business. Incidental personal use is permitted provided it does not interfere with the individual's business responsibilities, and provided it complies with all the rules set out in Electronic Communication and Social Media policy.

To summarise the use of emails:

Employees **should**:

- Have regard for the content and tone of their emails
- Be aware that an email is not always a substitute for a telephone or face to face conversation
- Verify and consider the appropriateness of recipients, especially when sending attachments with/without confidential information

Employees **should NOT** use:

- For any unlawful endeavour
- To use or transmit any copyrighted material in a way that would infringe the rights of the copyright holder
- To transmit threatening, insulting, sexually explicit, obscene, abusive, slanderous or otherwise inappropriate content

- To criticise any competitor or customer of the Company in a way which could damage their reputation
- to transmit any message which would constitute or encourage conduct viewed as criminal, give rise to civil liability, violate any local, national or international law, and/or impugn the good name and reputation of InHealth Group

28. Bring Your Own Device (BYOD) - Use of Non-TAC Equipment

Individuals (staff/contractors/suppliers) may need to use their own personal devices to access the TAC networks and information.
Any individual requiring this capability must notify TAC IT department of the equipment and intended use. Approval of use will depend on use and required level of access to TAC information and networks. Approval is required as all devices cache information without your knowledge, this could inadvertently lead to a data breach

As part of the approval for use process, staff and IT must both provide relevant assurance that the following key elements are present on any BYOD device:

- Secure Access Control (Password controlled)
- Encryption
- Up to date Anti-Virus/Malware Software

TAC reserves the right to refuse access where controls cannot be established or would be costly to do so.

Users wishing to use BOYD devices must:

- Make these available for investigation/audit upon request
- Provide all equipment used to be “cleaned” by the IT service department prior to leaving the organisation
- Allow software updates (e.g., encryption) onto devices at the discretion of TAC
- Ensure the data is secure at all times.

This will be under the provision that TAC will take no ownership or responsibility for any issues that may arise with equipment not owned by the business.

29. Electronic Information Storage

Information must be stored securely at all times. The specific controls will vary depending on the nature of the device. All access to electronic information is limited to only those that require it.

Should data need to be stored elsewhere on a short-term basis, this must be risk assessed and approved by TAC IT department and the following controls in place as a minimum:

- **Portable Media and Laptops** - Each device will be encrypted to allow storage of data for a short-term basis and must be transferred back to the original location as soon as is practicably possible

- **Desktop PC** – no data will be stored on individual desktop PCs (C\) without encryption storage. This will only be used for a short-term basis and must be transferred back to the original location as soon as is practicably possible

30. Encryption

Protection of confidential data while held and transferred electronically is a key area that must provide an additional layer of protection. To this end, an evaluation of risk should be undertaken when considering retaining/holding confidential data.
All confidential electronic data held/transferred by the TAC and its staff must be encrypted to the minimum standard specified within this policy. Use of any equipment of transfer without adequate encryption will be deemed as a negligent action by an employee and subject to disciplinary procedures.

The present standard is AES 256bit encryption as a minimum.

Passwords for encryption must meet those defined within the password section of this policy.

31. Protection against external and environmental threats

Inappropriate disclosure and breach of confidentiality and IT security has an increased risk when users fail to secure devices and information when not in use. The most common is at the users working space.

31.1 Clear Desk and Screen Policy

To protect personal and confidential data, TAC has a clear desk and screen policy.

- **Screens** - Users are expected to lock devices when away from the desk. (e.g., for desk computers and laptops - Windows Key & L).

  For clarity, the description of "away from desk" is defined as where the user is NOT in direct control of the device for any period of time.

- **Desks** - any sensitive, commercial or Personal information must be placed out of sight (i.e., in locked cabinets or drawers) when not in us and away from potential access by unauthorised persons.

31.2 Third Parties

Third parties (e.g., suppliers, contractors, customers, patients, etc.) should be challenged and verified by a receiving 'desk' before being granted access into a TAC facility. A log must be maintained of all visitors either in the form of a register or a patient daily list.

At points of service delivery to patients, personnel will ensure that patient identity is checked before any services are delivered.

Any third parties (e.g., IT contractors) requiring access to the information processing facilities shall be subject to the non-disclosure agreement as well as identity checks and IS induction as per employees.

31.3 Screening of Electronic equipment off premises

Clear direction regarding the use of electronic equipment (e.g., laptops) off- premises is given by the Mobile Device & Remote Working Policy

32. Access Controls and Passwords

All individual electronic information assets will have in place a process for the issue of unique access to each system. Access controls must be based on roles and responsibilities and limit access to only the functions and level of information required to fulfil their respective roles. The policy recognises that these will vary according to the system and technical requirements, but provides the following as a minimum standard that must be achieved:

33. Access Control

The access control processes will take account of security requirements of the system and will be granted only on documented approval of an application by the relevant system manager. The process must be:

1. Documented
2. Audited (reasonable level of compliance)

Access control covers both the setting up of users, but also deactivations when users change roles/leave. Access controls and procedures must ensure accounts are deactivated when a user no longer requires access to the system, but its history can remain in place in line with the records management policy for audit control purposes.

For all systems “Dormant” Access Control accounts will be deactivated after 3 months.

Generic accounts that do not allow unique access to systems as such will not be used in any of the systems/services used by TAC.

No individual will be given access to a live system unless trained and made aware of his or her security responsibilities.

34. Passwords

For those systems/services managed by TAC IT services and its IT providers, passwords used to access to electronic information assets they must meet the following specification:

- Are not names or have other connections to the user/system
- Be a minimum of 8 characters
- Are changed regularly (every 90 Days)
- Cannot be the same as the last 24 passwords
- Are a mixture of at least 3 of the following:
    - letters (CAPITALS and lower case),
    - numbers and
    - Special Characters
- Are not written down, shared or insecurely stored.
- Accounts must be locked out after 3 failed logon attempts

If a default password is used for accounts set-up by an administrator, the user must be prompted to change the password.

Where passwords have been intentionally given to other users, the account holder will be held responsible for destructive or illegal activity carried out by an unauthorised user to whom access has been given. Unauthorised access may contravene the Computer Misuse Act (1990) and Data Protection Act (1998) and other legislation leaving the user open to prosecution.

Legitimate Password Sharing

When sending information from one place to another in an encrypted form (e.g., unsecure email), the recipient must also have the password (key) to open the relevant information. In this circumstance you should still maintain the advice for strong passwords, but can release it, to the appropriate person.

35. Overriding Access Controls

In justifiable circumstances access to an individual's files, folders and systems will be granted to a line manager or investigating officer. This will only be authorised by written request from; the Caldicott Guardian (or nominated deputy) with HR approval. This will ensure that proper auditing of access made can be maintained and security of original user account is not compromised.

36. Anti-Virus and Spyware

Viruses, Worms, Trojan horses and hoaxes can potentially cause major disruption to our Business Servers, its clients and relationships with its clients. They can also prove costly to recover from.

The following measures are designed to manage the risk:

- Automatic virus detection software must be installed and kept up to date on every TAC PC and laptop.
- The workforce is responsible for immediately reporting any problems with their anti-virus software to the IT department.
- The workforce is responsible for immediately reporting all incidents where viruses are detected to the IT department with full details of the incident.
- The IT department is responsible for ensuring that updates to anti-virus software are made promptly available.
- Staff must not install or run unauthorised software (including games and screen savers) on any IT equipment owned by TAC.
- All files received or distributed by media must be scanned with anti-virus software prior to use.
- All servers connected to the live infrastructure must be protected by anti-virus software.
- Any client or third-party equipment that may occasionally be permitted to connect to the network must be checked prior to connecting to ensure it is free from viruses.
- Staff should not open emails that contain attachments if they do not know the source of that attachment or if they suspect malice.

What is a virus?

A computer virus is a programme that changes the way a computer behaves usually without the user's knowledge or permission and often copies itself to other computers. Non-destructive viruses may cause computers to behave in an unusual or unpredictable way.

Destructive viruses can destroy data and programs and can use the host computer to attack other computers.

Indications of a possible virus infection include:

- files or programmes corrupted or lost

- files increasing dramatically in size
- slowing of computer response time
- formatting of the hard disk
- unexpected text, visual or audio messages
- computer failure

What is a Worm?

Worms are similar to viruses. They spread by attaching themselves to files such as Word or Excel documents, screensavers and moving between computers when the file is transferred to another computer.

What is a Trojan horse?

A Trojan horse is a file that appears or claims to be useful or desirable but contains malicious code which, when opened or triggered, can:

- cause loss and theft of data
- pass the control of the computer to remote users
- use the host computer to attack other computers

What is a Virus Hoax?

Virus hoaxes are usually email messages that work in a similar way to chain letters. They warn of a new virus threat that does not exist. By forwarding the 'warning' to other users the hoax spreads misinformation and confusion. It may also increase email traffic as users email the warning to others.

If you receive an email advising you of a new computer virus do not forward the email on. Check with the TAC IT department who will advise whether it is a hoax or not.

Staff must be aware of computer viruses and contact the IT services if a virus incident is suspected.

Firewalls

The organisation will have in place suitable firewall(s) to prevent unauthorised network access to systems by external sources. This will be in place at all times and a process in place to authorise access accordingly, this will be managed by the IT service provider.

Any changes required to firewalls to allow access to the TAC networks must be requested via the IT services and approved prior to any changes.

Portable Data Storage Devices

TAC will monitor and restrict the use of Portable Data Storage Devices being attached to PCs/Laptops or other electronic equipment to ensure any transferred data/information to or from them is secure.

These devices include:

- USB Devices
- Memory Cards (SD/MMC etc.)
- IPads, Phones, Smartphone's, Blackberries
- CDs/DVDs/Floppy Disks/Storage Tapes

37. Penetration Testing

TAC will aim to have in place a programme of annual penetration testing to ensure IT infrastructure is appropriately secure. For the purpose of TAC infrastructure, this will be managed by the TAC IT department.

38. Application Security

This section applies to TAC internal applications.

An application, which processes sensitive data, or requires protection because of high measures of risk that could result from improper operation, manipulation or disclosure, must be afforded protection appropriate to its sensitivity.

The following are the minimum controls to be applied to sensitive applications, i.e. systems that contain or hold Sensitive Data or requires protection because of high measures of risk that could result from improper operation, manipulation or disclosure, with additional controls or safeguards to be imposed if appropriate:

- Security requirements and specifications will be approved by the TAC IT department prior to acquiring or starting development of applications, or prior to making a substantial change in existing applications.
- Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements.
- New or substantially modified sensitive applications shall be thoroughly tested prior to implementation to verify that the user functions and the required administrative, technical and physical safeguards are present and are operationally adequate.
- Live sensitive data or files must not be used to test applications until system integrity has been reasonably assured by testing with non-sensitive data or files.
- Sensitive applications will not be made live until the system tests have been successfully completed.
- Any sensitive software documentation should be provided the same degree of protection as that provided for the software.

39. Accreditation of Information Systems

TAC shall ensure that all new information systems, applications and networks include a security plan and are approved by the relevant committee before they commence operation to ensure this Information Governance & Security Policy has been applied.

40. Termination or Change of Employment

Reference: Access Control

The line manager shall advise HR, who will in turn notify IT Service Desk, of the time and date of an employee's departure or the time and date upon which an employee's access profile for both IT access and smart card should be disabled (whichever is the sooner).

The requirement to return company assets is clearly defined in the Contract of Employment and in HR policies. It is the line managers' responsibility to ensure assets are returned to the IT Service Desk asset where it is IT equipment, or the issuer if other company assets such as medical equipment.

41. Information Security in Projects or Change Management

Information governance and security related considerations should be a part of all project activity, for any project which requires a capital expenditure or involves significant business process change.

The primary considerations apply to:

- Changes to existing information flows, whether system and/or people based
- Development or modification of information systems
- Changes to organisational structures

42. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CGC to ensure this Information Governance & Security Policy has been applied.

43. Physical Security Controls

It is the responsibility of all TAC staff to make their area of work as secure as is reasonably possible.

44. General Physical and Environmental Security

All TAC premises (including those that are used by TAC but located outside of TAC offices) must be physically secure to prevent unauthorised access. Premises will have personnel at reception areas to check the legitimacy of all personnel entering the building.

All staff must observe and adhere to the security arrangements of the building in which they are working or visiting. Personal identity cards should be on display at all times while on site.

Visitors should be registered via SwipedOn and wait in reception until their host can escort them to their destination and back to reception when leaving.

If you have access to secure areas within TAC premises/areas of responsibility you should ensure that only yourself and approved staff have access to these areas and should not share entrance codes.

If you suspect someone is not a member of approved staff or a visitor, you should approach them. However, staff should ensure that they do not put your personal safety at risk, but report if necessary.

45. IT Server and Communications Rooms

All IT server rooms must be locked at all times. All Staff working in the IT server room must be trained on the fire prevention systems in use. Unrestricted access must be limited to those who regularly need it and that access reviewed on a regular basis.

Rooms containing ICT components such as servers providing network services, active network devices and patching for example, shall be contained in rooms that are locked at all times when not occupied

Critical and sensitive (NHS) ICT equipment will be protected by in a locked room with coded access.

46. Deliveries (equipment security)

IT equipment must be securely stored when delivered and signed for by Facilities/ IT department.

47. Cabling security

Desktop equipment should be secured in a manner commensurate with the risk of misuse, theft or damage. Power and telecommunications cabling carrying data or supporting information services shall be reasonably protected from interception or damage.

48. Secure disposal of IT equipment (including magnetic media)

All information held on any IT equipment must be securely destroyed by the TAC IT department prior to disposal or re-use of the equipment. Treatment of clients' information must follow written clients' instructions.

Returned PCs' hard drives must be completely wiped by the TAC IT department using a suitable security product.

49. Sharing of Personal Information and Transfer of Data/Information

The transfer of any physical confidential information must:

- Be reviewed and a lawful basis established to transfer it
- Follow the principles and underpinning guidance to maintain the security of the information in transit.

50. Data Flow Mapping

Routine transfers should be logged regardless of size to allow review of security procedures in place and compliance with Information Governance requirements. IAOs are required to identify and log the routine transfers of data that will take place including:

- Lawful basis
- Use of approved method
- Volume
- Frequency
- Risks
- Compensating controls

51. Printing

Data and information classified in accordance with TAC Information and Risk Management Policy must not be left unattended on, or nearby to, printers. Excess copies should be disposed of securely.

52. Secure Disposal of Information

52.1 Disposal of Manual Information
Manual information will be disposed of using certified confidential shredding services.

52.2 Disposal of Electronic Storage Media Information
Electronic assets - CDs, Memory Sticks, Hard Drives, Laptops, Desktop PCs, and Personal Data Assistant (PDA) etc. must be disposed of by IT services.

53. Support and Resources

TAC will ensure that any organisations from which it commissions its services will meet expected information governance standards as outlined in the contractual terms and conditions.

Clinical Services

All clinical services commissioned by or on behalf of TAC will be required to:

- Have a suitable contract in place to identify clear data controller relationship management in relation to the information required to effectively deliver and monitor commissioned services
- Ensure the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and security of information.
- Completion of the annual NHS Data Security and Protection Toolkit (with specific reference to the Information security standards) and undertake an independent audit to be disclosed to TAC on request to provide assurance they have met expected requirements
- Ensure privacy notices make individuals aware of TACs role in commissioning and the personal and sensitive data it may receive to undertake such a role
- Ensure that where any IG incidents occur that they are reported to TAC via routes determined within the contract
- Ensure the contract stipulates sufficient security controls to meet or exceed requirements set out in this policy.

Support services

All support services that process information on behalf of TAC will be required to ensure:

- The contract stipulates sufficient security controls to meet or exceed requirements set out in this policy
- A suitable contract is in place to form a Data Controller to Data Processor relationship where Personal Confidential data is managed on behalf of TAC
- Ensure the services commissioned meet the requirements of the Data Protection Act (and other legislation / directives) when providing services including but not limited to fair processing, maintaining adequate security of information and systems.
- Completion of the annual NHS Data Security and Protection Toolkit and undertake an independent audit to be disclosed to TAC on request to provide assurance they have met expected requirements.
- That any processing is within the remit of the contract or seek written confirmation if there is any ambiguity / change in service description
- Report any known incidents or risks in relation to the use or management of information owned by TAC.

54. Dissemination and Implementation

This policy is permanently available in our Integrated Quality Management System. Additionally, this is included in the Induction Process for all new starts and this policy will be included for reference where necessary.

The policy will be supported by additional related policies and resources to support implementation. This will include the availability of, and access to, written and verbal advice, guidance and procedures where necessary.

55. Training requirements

Information Governance & Security is fundamental in everyone's training, and a mandatory annual requirement.

For TAC, training will be provided in a 2-tier approach – Corporate (covering local variances, systems, passwords, access and familiarity with individual processes and systems) and Legislative (covering Information Governance, GDPR, Security principles)

For the corporate training this will be provided as part of the induction process. Whilst the Legislative will ensure staff and TAC understand their responsibilities and the consequences of not complying; refresher training will be undertaken annually.

56. Education and Dissemination

As executive lead for IG&S the Clinical Director has overall responsibility for ensuring this policy is implemented and disseminated.

The attention of staff will be drawn to this policy during Induction and it is available to all staff through our Integrated Quality Management System.

57. Monitoring and Review

Process for Monitoring Compliance

- Compliance with this policy will be undertaken by the Quality & Compliance Team and reported to the IRMG.
- Performance against the policy will be monitored against
- Availability and dissemination of policy and in alternative formats where requested or need identified
- Acceptance and understanding of audience (training, spot checks, surveys)
- Reports of non-conformance i.e. incidents or risks
- Compliance against the Information Governance Toolkit

This policy will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:

- Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risks or following significant incidents reported;
- Changes to organisational infrastructure.

Monitoring of individuals

To ensure compliance with the Law and organisational policies (including this one) TAC reserves the right to monitor usage and content where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)

- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

In addition, communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of TAC's business, and the employee's position within TAC. Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

This will include the use or access to any Network or where the property of TAC is used in the communication or is accessed remotely from outside the Organisation. This includes the use of portable computers and mobile devices such as work mobile phones/tablets etc.
Non-conformance with this Policy

Should it not possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the Quality & Compliance Manager. Any issues will need to be documented as a risk and either:

- Accepted and reviewed in line with this policy
- Accepted with a view to implementing an action plan to reduce the risk
- Not accepted and the practice will stop until such time as the risk can be reduced

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual.

These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Human Rights Act 1998
- Public Records Act 1958
- Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public has been reviewed in line with expected Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible, removing any disproportionate adverse impact on employees, patients and the public on the grounds of protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as "minimal impact".

APPENDIX A - EVALUATION PROTOCOL

Monitoring requirements	Aspect
'What in this document do we have to monitor'	The management of information risks (Information Risk Management) Compliance with the law Compliance with the Information Governance Toolkit Incidents related to the breach of this policy Destruction of Information Assets Registration of Data Flows and Information Assets Compliance with Registration Authority Terms and Conditions Monitoring of inappropriate access to systems (where possible)
Monitoring Method	Information Risks will be monitored through the Risk Register Compliance with law will be monitored through audit, work directed by the NHS Data Security and Protection Toolkit (DSPT). The NHS Data Security and Protection Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the DSPT will be audited by the organisation's internal audit function before the annual submission.
Monitoring prepared by	Q&C will produce incident reports
Monitoring presented to	Caldicott Guardian CGC
Frequency of Review	Yearly updates will be provided to the relevant groups, the CGC and the Caldicott Guardian Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system Annual (as a minimum) updates to the Board will be provided. The internal audit report on ISMS performance will be provided to the Board or delegated sub-committee by the CGC. Incident Reports will be reviewed as occurred and as directed by the seriousness of the incident

APPENDIX B - EQUALITY ANALYSIS

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

	Challenge questions	Yes/ No	What positive or negative impact do you assess there may be?
1.	Does the proposal affect one group more or less favourably than another on the basis of:	No	
	Race	No	
	Ethnic origin	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Disability	No	
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)	Yes	Improves work/life balance as opens more flexi working opportunities
3.	Will the proposal have an impact on social environment?	No	
4	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)	Yes	Improved home working and flexi-working opportunities
5	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)	Yes	Improved access

An answer of 'Yes' to any of the above question will require the Policy lead to undertake a full Equality & Equity Impact Assessment (EEIA) and to submit the assessment for review when the policy is being approved.

APPENDIX C - INFORMATION ASSETS

This is an illustrative list of the types of Information Assets TAC may hold

Personal / Other Information (to include Manuel and Electronic)	Software
• Paper Records and Reports (Patient/Staff/Clinical /Corporate) • Databases • System documentation • Process documentation • Back up and Archive Data • Audit Data • Patient case notes and staff records • Paper reports • Emails • Contracts	• Application Programs (Office 365) • System Software (e.g. Windows package) • Data Encryption Utilities • Development and Maintenance Tools • Cloud based systems (Cliniko, Xero etc)
Hardware	**People**
• PC's, Printers, copiers etc. • Laptop • Tablets • Phones • Removable Media (Pen sticks, External Hard Drives, etc) • Mobiles • Networks infrastructure and connections	• Qualifications • Experience • Skills • PDR's • Employment Position/Job Description • Absence records
Physical	**Services**
• Equipment (Clinical and Non-Clinical) • Furniture • Infrastructure • Buildings	• Lighting • Heating • Air-Conditioning • Lifts • Communications (e.g. telephone) • Power • Utilities • Wi-Fi

APPENDIX D – GUIDE TO CONDUCTING A PRIVACY IMPACT ASSESSMENT

Introduction

1. All organisations experience change in one form or another. Where a proposed change involves any form of information processing or storage it is important that our change procedures include an assessment of the potential impact on the confidentiality, security and accessibility of that information. This is formally called a Privacy Impact Assessment (PIA).

2. Before putting new processes in place, project and system sponsors should carry out a simple PIA as set out in this guidance. This will identify if there is a potential impact which will require more detailed analysis to be undertaken.

3. Confirmation that this aspect of change has been considered will be sought as part of the approval process for new business cases and systems.

Business Case Approval

4. Business cases submitted to TAC and THE Board include a requirement to answer the following statement:
   *This matter has been assessed for potential impact on personal data and privacy: Yes/N*o

5. Before answering YES to this statement sponsors of Business Cases should consider whether any changes proposed impact on any aspect of privacy, confidentiality or information security. They should consider the points outlined in appendix C1 to this policy and if there is a potential impact on our ability to comply fully with current legislation or guidance, they should seek advice from the appropriate Trust Information Governance lead. (See appendix C2 for contact details of leads)
6. Any risks identified as a result of the review will need to be dealt with in accordance with the procedure outlined in TAC Risk management strategy.

New System Approval

7. The introduction of new data handling or storage systems requires the approval of TAC CGC & IRMG

   The proforma, used to outline any proposal for new system developments or purchase, includes sections on Data Protection, Confidentiality and Security. The information included in these sections will identify any potential impact on privacy and confidentiality and these will be addressed as part of the Approval process.

Other Changes to Systems and Processes

8. In a bid to improve efficiency, reduce costs and update our technology we continually change and improve the way we work. Even minor changes to the way we process information can impact on our ability to keep information safe and secure, and comply with current legislation and best practice.

9. Technical changes and upgrades to core information systems will be subject to formal change control procedures managed IT PCL Technologies. For other changes and developments the points outlined at appendix 1 provide a reasonable checklist to assess if there may be an adverse impact on data protection confidentiality or information security as a result of any change. It

should be used before introducing any change in process and any issues arising from this outline review should be resolved before proceeding with any change.

Conclusion

Changes introduced to the way we handle information can adversely impact on data protection, information security and confidentiality. In order to ensure we remain compliant with current legislation and guidance sponsors of new processes and systems and staff introducing changes to processes and systems should consider the impact of the changes they are proposing.

Appendix E acts as a checklist of things that should be considered in relation to data protection confidentiality and information security. If the checklist indicates there may be a potential adverse impact arising from the change the matter should be raised in the first instance with the appropriate Information Governance specialist. If necessary, the issue will be considered by both the CGC & IRMG.

APPENDIX E – INFORMATION GOVERNANCE & SECURITY POLICY CHECKLIST

This checklist is intended to be a helpful Information Security aide-memoir for Staff. It is not intended to be a comprehensive summary of user responsibilities and does not reduce or alter the standards or principles in the Information Security Policy.

Staff should:

- ✓ Understand what information they use is:
    - Confidential - Personal
    - Confidential - Commercial
    - Open
- ✓ Speak with your line manager if you are aware that you are not meeting the standards and principles of the Information Security Policy
- ✓ Be aware of the potential risks that surround the data/information you use
- ✓ Safeguard portable IT equipment - do not leave them visible and unprotected in public places and certainly not signed in.
- ✓ Ensure portable hardware is encrypted
- ✓ Follow password protection guidance
- ✓ Dispose of any confidential electronic or paper data/information securely
- ✓ Log off or lock computers if you are not using them (Windows Key + L)
- ✓ Wear your staff identification badge at all times
- ✓ Report all incidents using the Incident Reporting Form appropriate mechanisms

Staff must not:

- X Move any non-portable IT equipment without contacting the Helpdesk
- X E-mail Sensitive, Personal or Commercial information without following the Computer and Mobile Phone Acceptable Use Policy
- X Share passwords or use someone else's password
- X Copy personal data from one system to another without confirming that the recipient system has the same or greater security protection
- X Use or try to use IT networks which you have not been authorised to use
- X Copy software without the authority of the copyright holder
- X Store confidential information on portable IT equipment such as Laptops and Pen drives without encryption being used
- X accessing Company networks from internet cafes or external public places

APPENDIX F - INCIDENT RISK MANAGEMENT GROUP TERMS OF REFERENCE

1. Purpose of Group

1.1. The IRMG is established to:

1.1.1. Provide policy direction and guidance to TAC on Information Governance related procedures and issues.

1.1.2. Prepare the annual submission of the NHS Data Security & Protection Toolkit.

1.1.3. Develop and implement a strategy to lead and improve standards of Information Governance across TAC.

2. Specific Responsibilities and Scope of Group

To develop an IG policy and associated IG strategy and maintain the currency of the policy.

2.2. To prepare the NHS Data Security & Protection Toolkit (DSPT) assessment for sign off by TAC CGC on behalf of the Board.

2.3. To develop and lead TAC's Information Governance work programme.

2.4. To review reports and other documentation produced relating to IG.

2.5. To ensure that TAC's approach to data/information handling is communicated to all staff and made available to the public.

2.6. To coordinate the activities of staff with data protection, confidentiality, information security, data quality, records management and freedom of information responsibilities in their job responsibilities.

2.7. To provide assurance that the relevant policies and procedures are in place to ensure compliance with the law and guidance in respect of information handling.

2.8. To ensure that appropriate training is provided to Trust staff as necessary to support their role and obligations in respect of Information Governance.

2.9. To develop and implement procedures to ensure new or proposed changes to organisational processes or information assets that may impact on Information Governance are identified and assessed. Provide a focal point for the resolution and/or discussion of Information Governance issues.

3 Membership

The IRMG core membership will comprise:

- Q&C Manager
- Q&C Assistant Manager
- Clinical Director (or rep)
- Chief Nurse
- IT
- OH
- HSSE & F Manager
- Admin Manager

3.2 Other individuals may be invited to attend specific meetings to advise on areas of expertise

3.3 The Chair will follow up the repeated non-attendance of any group members.

4. **Frequency** of Meetings

4.1. Meetings will be monthly.

5. Quorum

5.1. For the group to be a quorum there must be 4 members present including either the Q&C Assistant/Manager as Chair or Clinical Director (rep).

6. Accountability

The IRMG is accountable to CGC.

7. Reporting

7.1. Information governance will be a standing agenda item at meetings of ISSG.
7.2. The annual submission of the NHS Data Security & Protection Toolkit will be approved by CGC before submission.

8. Review

The group will review these terms of reference annually in JANUARY of each year