Appendix A – Information Governance Management Framework –

NHS Shropshire, Telford and Wrekin ICB

	Requirement	Detail
Senior Roles within the ICB	**Chief Executive:** Simon Whitehouse, Interim Chief Executive	The Chief Executive of the ICB has overall accountability and responsibility for Information Governance in the ICB and is required to provide assurance through the Annual Governance Statement that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
	Senior Information Risk Owner and Executive IG Lead: Claire Skidmore,	The Senior Information Risk Owner (SIRO) is an Executive Director of the ICB Board. The SIRO is expected to understand how the strategic business goals of the ICB may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions and will provide written advice to the Chief Executive on the content of their Annual Governance Statement in regard to information risk. The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Chief Executive are kept up to date on all information risk issues. The role will be supported by the Midlands and Lancashire Commissioning Support Unit Information Governance Team and the Caldicott Guardian, although ownership of the Information Risk Agenda will remain with the SIRO.

	Requirement	Detail
		The SIRO will be supported through a network of Information Asset Owners and Assistants who have been identified and trained throughout the organisation. The SIRO is also appointed to act as the overall Information Governance lead for the ICB and co-ordinate the IG work programme. The Executive IG Lead role has been assigned as Department of Health response to the Caldicott 2 Review contains an expectation that organisations across health and social care strengthen their leadership on information governance. The Executive IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG, although the key tasks are likely to be delegated to an Operational IG Lead.
	Caldicott Guardian: Nick White Chief Medical Officer	The Caldicott Guardian has particular responsibility for reflecting patients' interests regarding the use of patient identifiable information and to ensure that the arrangements for the use and sharing of clinical information comply with the Caldicott principles. The Caldicott Guardian will advise on lawful and ethical processing of information and enable information sharing. They will ensure that confidentiality requirements and issues are represented at Board level and within the ICB's overall governance framework.

	Requirement	Detail
	Data Protection Officer: Hayley Gidman Information Governance Lead (MLCSU)	The Data Protection Officer (DPO) reports to the SIRO. This ensures the DPO can act independently, without a conflict of interest and report direct to the highest management level. The DPO is responsible for ensuring that the ICB and its constituent business areas remain compliant at all times with data protection, privacy & electronic communications regulations, freedom of information act and the environment information regulations. The DPO shall lead on the provision of expert advice to the organisation on all matters concerning the information rights law, compliance, best practice and setting and maintaining standards.
	MLCSU Information Governance Lead: Hayley Gidman Information Governance Lead (MLCSU)	The key purpose of the role is to ensure the ICB successfully achieves the required level of compliance across all requirements of the NHS Digital Information Governance Toolkit. The post holder will support the ICB to ensure the establishment of corporate standards and a consistent ICB wide approach to Information Governance and will be responsible for assuring the implementation of a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance.
	Information Governance Organisational Lead: Sara Spencer, Operational IT & IG Lead	The key purpose of the role is to ensure the ICB successfully implements a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance with Information Governance & Information Security. The post holder will ensure the

	Requirement	Detail
		implementation of corporate standards and a consistent organisation wide approach to Information Governance & Information Security.
Key Governance Bodies A group, or groups, with appropriate authority should have responsibility for the IG agenda.	**Audit Committee**	The Audit Committee is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance in the ICB.
Resources Details of key staff roles	**Dedicated MLCSU Information Governance Staff**	Information Governance Consultant Name: Jade Goodwin Email: jade.goodwin3@nhs.net Senior Information Governance Consultant Name: Pippa Joyce Email: pippa.joyce@nhs.net Head of Information Governance Name: Hayley Gidman Email: Hayley.gidman@nhs.net
Governance Framework Details of how responsibility and accountability for IG is cascaded through the organisation.	**Information Asset Owners**	Information Asset Owners are senior individuals involved in running the relevant business. The IAOs role is to: • Understand and address risks to the information assets they 'own'; and • Provide assurance to the SIRO on the security and use of these assets. Information Asset Owners have been nominated across the whole organisation and have received specialist information risk training to allow them to be effective in their role.

	Requirement	Detail
	Information Asset Administrators/Assistants	The Information Asset Administrators/Assistants role is to: • Ensure that policies and procedures are followed • Recognise potential or actual security incidents • Consult their IAO on incident management • Ensure that information assets registers are accurate and maintained up to date. Information Asset Owners have received specialist information risk training to allow them to be effective in their role.
	Employment Contracts	All staff and those undertaking work on behalf of the ICB need to be aware that they must meet information governance requirements and it is made clear to them that breaching these requirements, e.g. service user confidentiality, is a serious disciplinary offence. This is supported by the inclusion of clauses within staff contracts both for substantive and temporary staff that cover Information Governance standards and responsibilities with regard to data protection, confidentiality, and information security.
	Contracts with Third Parties	The ICB must ensure that work conducted by others on their behalf meet all the required Information Governance standards. Where this work involves access to information about identifiable individuals it is likely that the ICB will be in breach of the law where appropriate requirements have not been specified in contracts and steps taken to ensure compliance with those requirements. Therefore, the ICB endeavours to ensure that formal contractual

	Requirement	Detail
		arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.
Training and Guidance Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The approach to ensuring that all staff receive training appropriate to their roles should be detailed.	**Information Governance Handbook**	Purpose of the Handbook: • To inform staff of the need and reasons for keeping information confidential • To inform staff about what is expected of them • To protect the organisation as an employer and as a user of confidential information The Handbook has been written to meet the requirements of: • The Data Protection Act 2018 • The UK General Data Protection Regulations 2021 • The Human Rights Act 1998 • The Computer Misuse Act 1990 • The Copyright Designs and Patents Act 1988 • A Guide to Confidentiality in Health and Social Care (NHS Digital) The Handbook has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. If the Handbook is breached, then this may result in legal action against the individual and/or organisation as well as investigation in accordance with the organisation's disciplinary procedures.
	Training for all staff	All staff receive basic IG Induction training online via Teams Refresher training will be via ESR online.

	Requirement	Detail
	Specialist IG training	Specialist IG training is provided across the organisation for those staff that are given additional responsibility for IG within their areas. Current specialist training includes: • Information Risk Training • DPIA • FOI • SAR
Incident Management Clear guidance on incident management procedures should be documented and staff should be aware of their existence, where to find them, and how to implement them.	**Documented Procedures and Staff Awareness**	Incident Management in the ICB is covered in the following organisational policies and Procedures: • IG Data Protection and Security Policy • IG Handbook Staff awareness is raised through the following ways: • Staff Induction • Information Governance Training • Incident Risk Training

Information Governance Management Framework