NCEPOD

NCEPOD Information Governance Management Framework

Version Control

Version Number	Date of change	Items changed	Changes made by	Sign-Off by Chief Executive
1.1	February 2010	Information Asset Register section added	RA	M. Ma
1.2	July 2013	Updated Governance roles and descriptions	RA	M. Ma
1.3	November 2013	Improved diagram quality. IAA definition added. Additional grammar corrections	RA	M. Ma
1.4	August 2015	Added Child Health Project Manager to document	RA	M. Ma
1.5	March 2018	Added reference to the GDPR and role of Data Protection Officer	RA	M. Ma
1.6	February 2020	Child Health Project Manager deleted	NS	M. Ma

Introduction

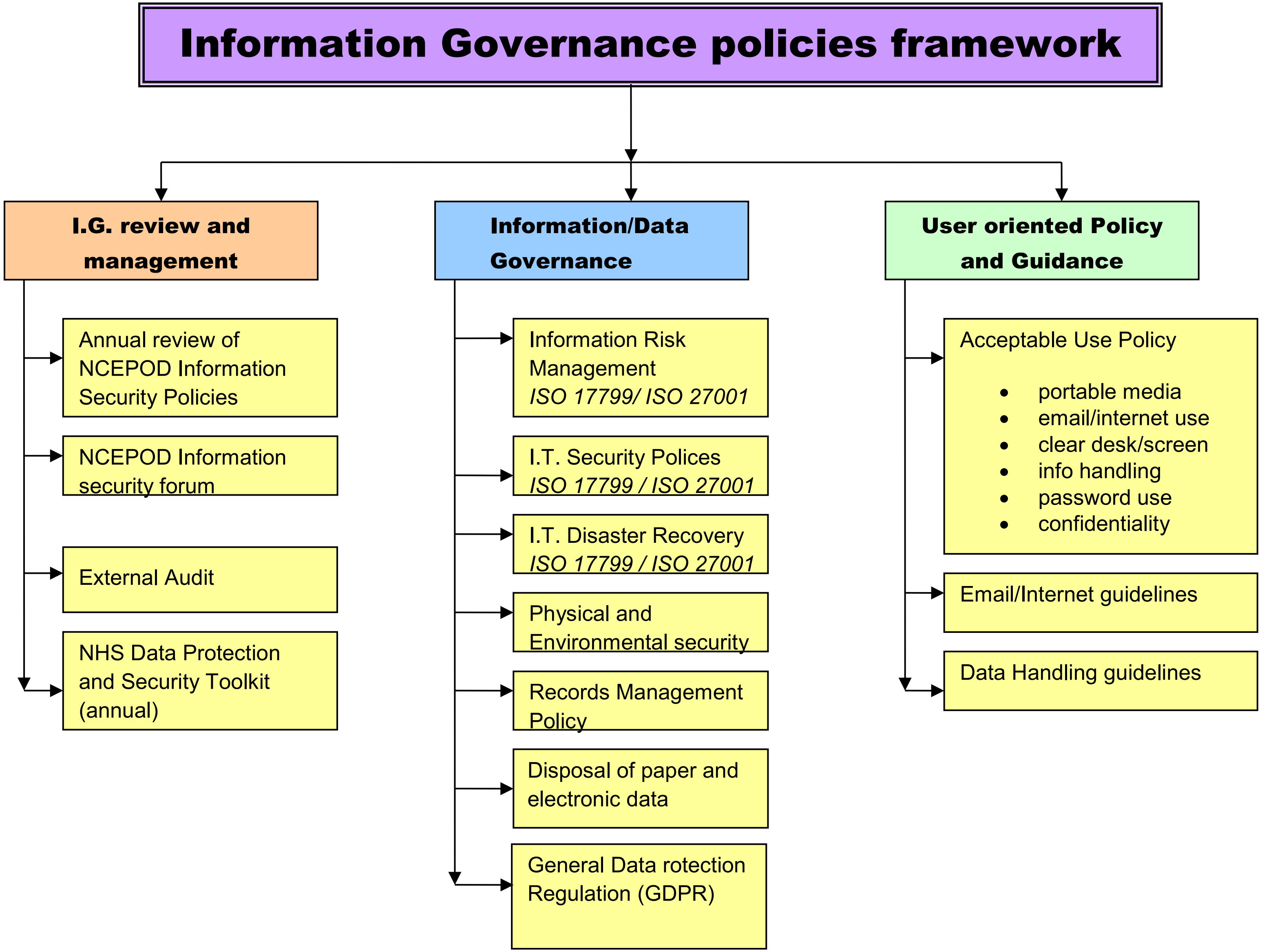
Information Governance (IG) requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

NCEPOD's own Information Governance Management Framework ensures the primary objectives of Information Governance are achieved:

- Information will be organised and managed in accordance with mandated and statutory standards and kept confidential.
- The integrity of information is assured, monitored and maintained, to ensure that it is of good quality and reliable for use for the purposes that it is collected and used for.
- Information required for operational purposes is kept secure and available to those who need it as part of their role.
- Compliance with legal and regulatory frameworks is achieved, monitored and maintained.
- All staff will have access to regular information governance training to ensure they understand their personal and organisational responsibilities for managing information and how to follow appropriate legislation.
- An information risk management strategy is implemented to ensure ownership of and accountability for NCEPOD's information assets and the mitigation of associated risks.

Information Governance polices framework

The diagram below shows the IG policies framework at NCEPOD. It categorises the management, governance, and guidance of information within NCEPOD, and the Information Governance functionality it undertakes.



Information Governance policies framework

I.G. review and management

- Annual review of NCEPOD Information Security Policies
- NCEPOD Information security forum
- External Audit
- NHS Data Protection and Security Toolkit (annual)

Information/Data Governance

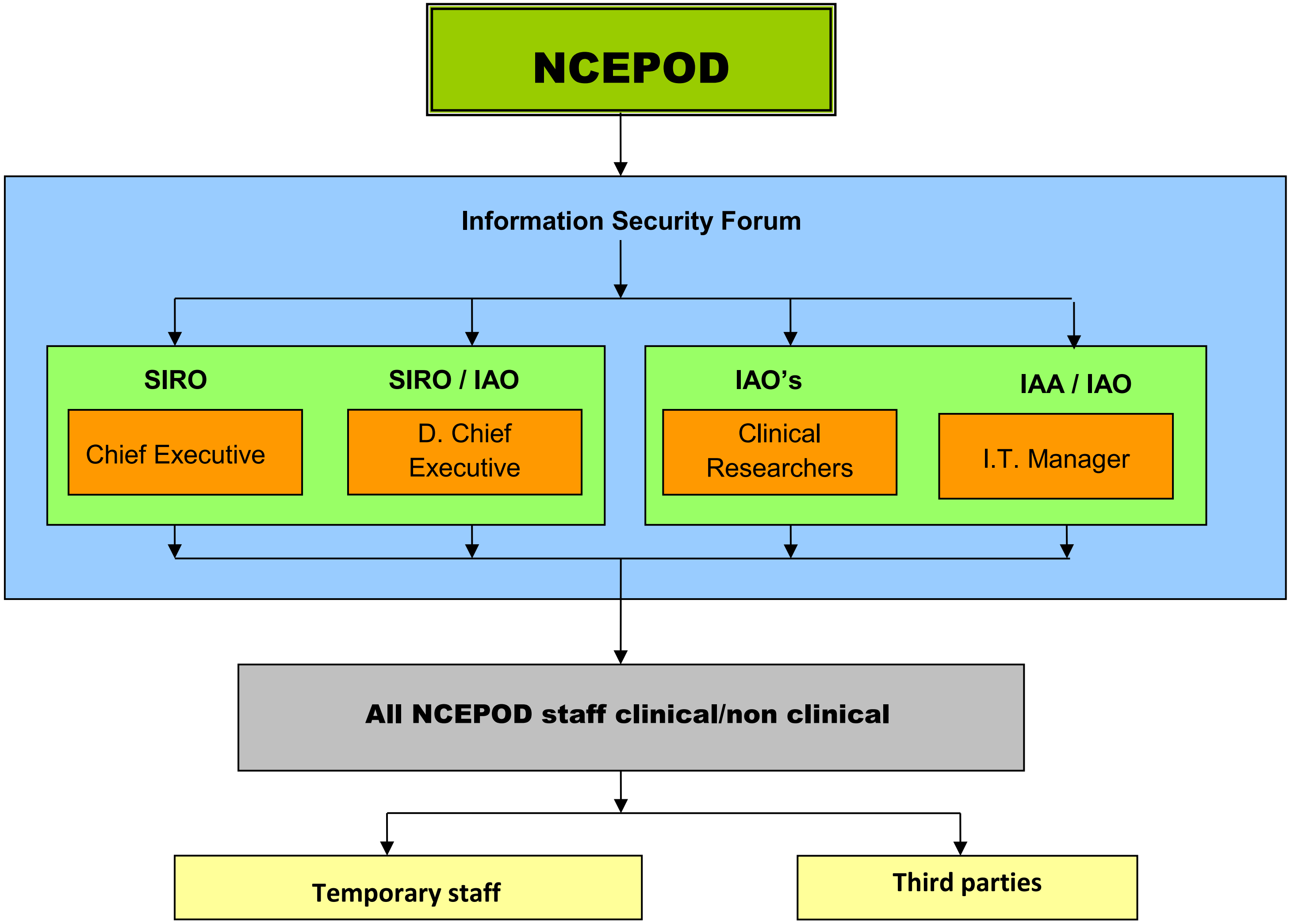
- Information Risk Management *ISO 17799/ ISO 27001*
- I.T. Security Polices *ISO 17799 / ISO 27001*
- I.T. Disaster Recovery *ISO 17799 / ISO 27001*
- Physical and Environmental security
- Records Management Policy
- Disposal of paper and electronic data
- General Data rotection Regulation (GDPR)

User oriented Policy and Guidance

- Acceptable Use Policy
  - portable media
  - email/internet use
  - clear desk/screen
  - info handling
  - password use
  - confidentiality
- Email/Internet guidelines
- Data Handling guidelines

Information Governance roles at NCEPOD

The diagram below shows the information governance roles for all members of staff within NCEPOD.



Information Security Forum

This forum consists of senior members of staff at NCEPOD, and they hold responsibility for ensuring the Information Governance function is addressed properly.

Chief Executive

Has overall accountability and responsibility for Information Governance within NCEPOD, and signs-off those decisions regarding Information Governance made by members of the IS forum.

Caldicott Guardian & Data Protection Officer

The Chief Executive is the Caldicott Guardian and the Data Protection Officer. As such they are the "conscience" of NCEPOD, providing a focal point for patient confidentiality and information sharing issues and advising on the options for lawful and ethical processing of information as required.

The Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for managing information risk within NCEPOD. This is undertaken by the Chief Executive or the Deputy Chief Executive (in the absence of the CEO) whose role is responsible to the NCEPOD Trustees for ensuring that all information risks are recorded and mitigated where applicable. The Chief Executive also holds overall responsibility for the Information Asset Register, in ensuring it is up to date and accurate. This task is delegated to the IT Manager who acts as the Information Asset Administrator (IAA).

Information Asset Owners (IAO)

Information Asset Owners are senior members of staff who are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.

Information Asset Administrator (IAA)

The role of Information Asset Administrator has the responsibility for ensuring information assets are correctly identified and recorded on the asset register, with an assigned asset owner responsible. The role also keeps the asset register up to date. The task of IAA is undertaken by the IT Manager.

Information Asset Register

All assets should be clearly identified and a register of all important assets drawn up and maintained. This register is located on the company network in digital format, and paper copy kept with the information security procedures document.

It will be the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented on the Information Asset Register which forms part of responsibility of the IAA.

The asset register should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, and a business value. The register should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned. In addition, ownership should be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified as should details of risk assessor, risk assessment frequency, risk assessment rating and date of last risk assessment.

There are many types of assets, including:

- information: databases and data files, contracts and agreements, system documentation, research information, business continuity plans and archived information;
- software assets: application software, system software, development tools, and utilities;
- physical assets: computer equipment, communications equipment, removable media, and other equipment.

N.B. Priority must be given to information assets that comprise or contain personal information about patients or staff.

The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; defining and periodically reviewing access restrictions, classifications, and business continuity arrangements taking into account applicable access control policies.

Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis (i.e. an information assets administrator (IAA)), but the responsibility remains with the owner.

The Information Asset Register is kept in a digital format, and held on NCEPOD's intranet.

Information Risk

NCEPOD establishes clear lines of accountability for information risk management that lead directly to the SIRO and the appointment of Information Asset Owners' (IAO) and an Information Asset Administrator (IAA) who is responsible for the maintenance of the Information Asset Register.

The IAO's and IAA roles are accountable to the Chief Executive for the management and mitigation of information risks and will provide assurance to that effect.

The IAO will ensure that information risk assessments are performed annually on all information assets where they have been assigned 'ownership' of. They will ensure that any significant risks are documented through the quarterly Information Security Forums meetings to the IAA and SIRO.

At least once a year, each of the IAOs will carry out a risk assessment to examine forthcoming potential changes to accessing the information they oversee. These are carried out through the life of each project each of the IAO's undertakes.

The SIRO and Information Security Forum will be made aware of all information risk assessments and approve identified risk mitigation plans.

Confidentiality Code of Conduct

All staff, whether permanent, temporary or contracted, are aware or their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality. Failure to maintain the above may lead to disciplinary action, including dismissal.

Training and Development

Fundamental to the success of delivering the Framework is maintaining an Information Governance culture within NCEPOD. Awareness and training needs is available to all staff, who utilise information in their day-to-day work, to promote this culture.
All staff should receive annual basic information governance training appropriate to their role within NCEPOD. A register of this is kept with all staff records.
Senior staff must also undertake further training using the online NHS Information Governance Training Tool from which they can train the other members of staff within their daily roles.

All new staff are explained the principles of Information Governance within their induction process and have to read the Information Security Procedures.