

# Information Risk Management Policy

## 1. Purpose

This policy and its sub policies and associated procedures define how the British Library will manage information risk. It is intended to ensure that all security, compliance and other risks to the British Library's corporate information are identified, analysed and managed so that they are maintained at acceptable levels. This includes risks to the confidentiality, integrity and availability of Library information.

This policy lays the framework for a formal information governance programme (focusing primarily on risks to information assets) by establishing responsibility for risk mitigation, programme management and oversight of the information policy framework.

The policy fits within the Library's overall business risk framework, and will need to be read in conjunction with the corporate Risk Management policy and processes.

## 2. Scope

This policy applies to all British Library Directorates, their staff (employed, contract or volunteer), and third parties that collect, transmit, retain or use for any purpose information on behalf of the Library in any form.

## 3. Statement of intent

The Library will identify and manage information risks that endanger the achievement of the strategic aims defined in its Business Plan or the operational aims defined in Directorate plans.

The Library will embed information management into business processes and functions by means of approved procedures, processes, and controls. Action taken to manage information risk will address issues relating to information compliance, information management, and information security.

The Library will make all reasonable efforts to discharge any information risk, management or security related obligations arising from legislation, regulation or voluntary agreement, drawing on best practice and recognised standards where appropriate. The Library will manage information in ways that support the efficient and effective achievement of the Library's strategic and operational aims, drawing on best practice and recognised standards where appropriate. The library will publish sub-policies, mandatory procedures and optional guidelines in support of this policy.

#### **4. Policy ownership**

The Senior Information Risk Owner (SIRO) owns this policy on behalf of the Library's Executive Team (ET). The SIRO, leading the Corporate Information Governance Group (CIGG), will be responsible for developing and implementing this policy and its associated sub-policies, and for reviewing them regularly to ensure that they remain appropriate to the Library's objectives and risk environment.

Changes, amendments or accepted deviations from this policy can be authorised only by the SIRO.

#### **5. Responsibilities**

Everyone in the Library has a role in the effective management of information. All staff should actively participate in identifying potential risks to the Library's information in their area and contribute to the implementation of appropriate solutions.

The SIRO and CIGG, in conjunction with the Integrated Risk Management Team (IRM), will be responsible for maintaining the currency of all aspects of this policy and its related sub policies, procedures and guidance, taking into account legal compliance, government directives and corporate strategies and resources.

The SIRO will act as an advocate for information security and risk to ET and in internal discussions, and provide written advice to the Chief Executive for the annual Statement of Internal Control relating to information risk for reporting to the DCMS.

#### **6. Assessment of information risks**

Information risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take based on the value of the information resource to the organization.

Identification and a threat assessment of risks related to the Library's information assets will be carried out in line with the corporate Risk Management policy and the Strategic Risk Register maintained by IRM, including an assessment of risk appetite and risk tolerance.

The SIRO will own the high level strategic information risk that is held on the Strategic Risk Register. This strategic risk recognises that an information related incident may cause serious harm to the Library, and that the risk of such an incident may arise from weaknesses in information governance structures, inadequate control of information content, inability to access information in a timely fashion, and/or inappropriate disclosure of information.

In turn CIMU will manage CIGG's Risk Register of more detailed risks related to each area of potential failure.

#### **7. Sub policies, procedures and guidelines**

Sub-policies, mandatory procedures and optional guidelines will detail the Library's approach to managing various aspects of information risk relating to information compliance, information management and/or information security.

## **8. Incident management**

Security breaches, information loss or unauthorised disclosure, and other risks associated with information management will be managed as 'incidents' with appropriate actions undertaken in terms of escalation, reporting, recovery and subsequent review of existing controls, policy and procedures.

## **9. Cultural change**

ET and the Board recognise that in order for information risks to be effectively managed there will, in some cases, be a requirement for cultural change and changes to current working practice within the Library. The SIRO and CIGG have been empowered by ET to develop and implement necessary changes to working practice to ensure that this policy (and its associated sub-policies) can be fully implemented.

The SIRO and CIGG will work closely with HR and Internal Communications to ensure that appropriate actions are taken to provide staff with adequate training and education in order that they can fulfil their requirements to implement, maintain and develop effective information management controls.

Failure to observe this policy (and its associated sub policies and related mandatory procedures) may be regarded by the Library as gross misconduct. Disciplinary procedures may be instigated as a consequence of damage caused to an individual, the Library or its partner organisations by non-compliance with this policy.

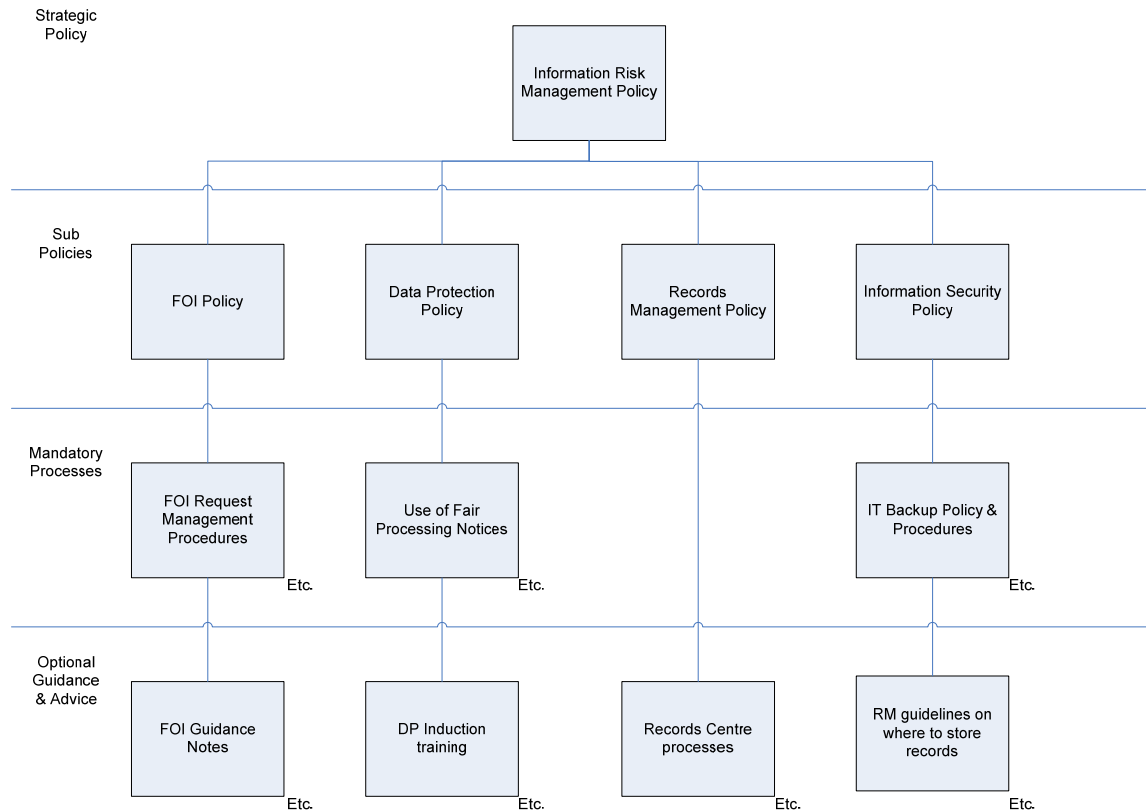
## **10. Monitoring and review**

The SIRO and CIGG will be responsible for monitoring the implementation of actions taken to implement the requirements of this policy. These actions will each be led by a sub-group or designated individual of CIGG. These specific actions will be monitored by CIGG on a regular basis.

The policy itself will be subject to annual review, or earlier if warranted by regulatory, statutory or policy change. The SIRO and CIGG will carry out the review.

## Annex A: Theoretical Policy Framework

The policy is conceptualised as an ‘umbrella’ policy that sits over the more detailed sub-policies that set out how the Library will manage various aspects of Information Compliance, Information Management and Information Security. Below these lower level policies will sit levels of mandatory procedures and optional guidance that cover the operational management of specific areas of risk such as PCI compliance, password management or data sharing, for example.



As such the IRM policy defines the role of the SIRO and CIGG, sets out the Library’s high level intent to manage information risk and the framework for doing so, and points to the lower level policies for specific implementation of the policy.

It is our intent that the policy be as short as possible whilst still containing enough detail to comply with the Cabinet Office Guidance on the Department Information Risk Policy.