OVERARCHING POLICY FRAMEWORK FOR SECURITY AND INFORMATION GOVERNANCE

Version 1.0

November 2018

ROYAL borough of GREENWICH

	Owner (Responsible for Approval of Issued Versions)		
Role	Signature	Date	Issue

Revision History:

Date	Version	Reason for change	Author
01/10/2013	V 0.1	Revised version of new policy document. This also incorporates the previously separate 'Policy approval process' document.	Jeremy Tuck
11/01/2013	V 0.2	Incorporated comments made by Jules Spain and the Information Governance Steering Group	Jeremy Tuck
21/01/2013	V 0.3	Incorporated comments made by Robin Clarke and following a further revision. Revised the title of the document	Jeremy Tuck
29/01/2013	V 0.4	Incorporated comments made the Information Governance Steering Group	Jeremy Tuck
15/11/2013	V 0.5	Incorporated the updated ICT policies	Jeremy Tuck
06/01/2014	V 0.6	Made changes to IGWG and updated the policy listing. Updated text related to Communications and Data Audits.	Jeremy Tuck
26/3/2014	V 0.7	Amendments	Jules Spain
06/11/2015	V 2.0	Formatting and review	
02/05/2018	V 2.1	Amendments	Doug Plumer
13/11/2018	V 1.0	Minor amendments, re-version for publication	Doug Plumer

Distribution:
This document has been distributed to:

Date	Version	Distribution
01/10/2013	V 0.1	Information Governance Working Group
11/10/2013	V 0.2	Information Governance Working Group
21/10/2013	V 0.3	Information Governance Working Group
29/10/2013	V 0.4	Information Governance Working Group
15/11/2013	V 0.5	Information Governance Working Group
06/01/2014	V 0.6	Information Governance Working Group
26/3/2014	V 0.7	Information Governance Steering Group

TABLE OF CONTENTS

1 PURPOSE 4
2 THE POLICY FRAMEWORK 4
3 POLICIES, STANDARDS AND CONTROLS 5
4 PEOPLE AND GOVERNANCE 5
5 MEASURES IN PLACE FOR ASSURANCE 6
6 CHANGES, APPROVAL AND REVIEW OF POLICIES 8

1 Purpose

This document is the Overarching Policy Framework for Security and Information Governance arrangements for the Royal Borough of Greenwich. It describes the framework within which the Council will promote a culture of good practice around the handling and processing of information, as well as the organisational structure and policies for achieving this.

2 The Policy Framework

2.1 Overarching commitment

The Council is committed to putting the customer at the heart of what it does. This is a fundamental principle to the way the Council handles customer data, sensitive personal data, and other important data in Council systems. Council staff are committed to deliver their duties in a way that is service-driven and remains customer focused, and to ensuring all data is:

- **Accurate** – services delivered and decisions made by the Council will be based on current and accurate information;
- **Confidential** – data will only be available to staff that have a valid reason for accessing that information;
- **Managed** – staff who access personal information will be aware of their responsibilities and obligations;
- **Available** – information will be available to authorised individuals where and when needed; and
- **Well-Handled** – stored, maintained, shared and disclosed in accordance with applicable legislation.

2.2 Who do these policies apply to?

People: Users of Council information and/or systems including permanent, contract and temporary Council employees, Council Members and 3rd party organisations who have been authorised to access and use such information and/or systems.

Information: Information and data collected, held or accessed in relation to Council activity whether by Council employees or individuals and organisations under a contractual relationship with the Council. Information stored on facilities owned or managed by the Council or on behalf of the Council. Information shared with, or entrusted to the Council by partners, clients or service users.

Systems: Information Systems within the organisation (both electronic and paper based) fall within the scope of this Policy.

2.3 Embedding the Governance Framework

The Governance Framework will be reinforced by relevant information governance and confidentiality clauses in staff contracts or Codes of Conduct and in the contracts of 3rd party and support organisations that may be involved with accessing personal data or the networks holding or carrying such data. Compliance is mandatory and contracts will include appropriate sanctions for non-compliance. Information Governance responsibilities are implicit where staff are responsible or accountable for managing information.

Access to systems, networks and information will be subject to monitoring and may be reviewed or audited at any time. Access logs will be retained to facilitate investigation in the event of an incident. Information shared with partner organisations will be subject to Information Sharing Protocols or agreements that will be developed and agreed on a case-by-case basis depending on the purpose, scope and scale of the information shared.

3 Policies, Standards and Controls

The Royal Borough of Greenwich recognises that its security and information governance arrangements need to support and integrate with other corporate policies, standards and controls. Therefore, the Council's security and information governance documentation operates within this context and is mindful of the existing arrangements for managing business continuity and strategic risks, governance and assurance and HR processes. This framework is underpinned by specific policies, standards and controls in relation to:

- Information management
- Using and accessing information systems at on-premises sites and remotely
- Working with personal and sensitive data
- Control of the ICT infrastructure

4 People and Governance

4.1 Senior Information Risk Owner

The Director of Finance serves as the Council's named Senior Information Risk Owner (SIRO) in relation to information governance and security related matters. The SIRO understands the strategic business goals of the Council and how business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance risk assessment and management processes within the Council and advises the Greenwich Management Team on the effectiveness of information risk management.

4.2 Information Governance Lead

This role, held by the Corporate Data Guardian, will be responsible for co-ordinating the Information Governance work programme and will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance.

4.3 Information Governance Steering Group

The Information Governance Steering Group (IGSG) will be chaired by the Information Governance Lead and is responsible for ensuring that appropriate information governance arrangements are in place throughout the Council in line with national standards.

4.4 Caldicott Guardian

Effectively the conscience of the Council, this role advises Senior Management on the handling and protection of personal and sensitive service user information. The Caldicott Guardian addresses information throughout Adult and Children's Social Care and Public Health. The

Caldicott Guardian is supported by Caldicott Guardian Officers, which are usually departmental managers in Adults, Children's Social Care, and Public Health.

4.5 Information Asset Owners

Information Asset Owners are responsible for ensuring at a service level that access controls are established to ensure that their information is only available to those with an identified business need. Information Asset Owners will also ensure that the information for which they are responsible is appropriately protected throughout its lifecycle while held within the Council and when shared with other organisations.

4.6 Key Supporting roles

There are specific information management roles in place to support staff in the areas of Data Protection, Freedom of Information and Records Management.

4.7 Staff responsibilities

Staff are responsible for complying with policies and for reporting information security incidents or issues. Staff are responsible for responding to information requests relating to their work as part of their day-to-day function. As part of this, staff must be aware of how to deal with information requests under the Freedom of Information Act and the Environmental Information Regulations and requests for personal information under GDPR and the Data Protection Act.

5 Measures in place for assurance

5.1 Overview

Information assurance describes the measures that are in place to ensure that the Council meets the requirements for good information governance. This section, therefore, describes how the roles and governance arrangements will operate to ensure that this is achieved.

5.2 The Information Governance Steering Group

The Information Governance Steering Group will oversee the development and implementation of the Information Governance improvement plan and monitor risks and issues relating to improved data assurance, records management processes. Actions arising will be formally agreed and managed through the improvement plan.

5.3 Staff training

Relevant staff will be trained on data handling, security and appropriate information governance. Training will be directed by the IG Steering Group, who will ensure there is an auditable record of training completion. Training will be appropriate to the requirements of the job role; however, key information will be provided at employee induction and a corporate e-learning tool will provide staff with a foundation in the key legislative, policy and behavioural requirements. Staff with access to personal information will be provided with guidance on expected practices relating to handling, disclosing and sharing this information. Other specific requirements will be assessed during appraisal by departmental managers. Specialist training will be provided for those staff with

Information Governance responsibilities, which may include use of the HSCIC IG Training Tool. Training records will be held by Learning and Development.

5.4 Promoting the awareness of information governance

There will be an on-going process maintaining good awareness of information governance matters throughout the organisation. Both passive and active awareness methods will be used: Passive awareness – Documents available and accessible on the intranet; and Active awareness – Briefings, emails, meetings, documents requiring formal acknowledgement. Policies, procedures, guidance and other supporting information are published on the Council's intranet, and when new documents are produced or existing documents updated, the relevant staff will be formally advised through management and departmental briefings or emails. In the case of key documents, staff may be required to acknowledge their understanding of the document and their obligations.

5.5 Incident Management

Information security incidents, breaches or weaknesses will be reported to the Service Desk in accordance with the Council's Information Security Incident Management Procedure. Information Security incidents will be passed to an Information Security Officer for investigation and resolution and will be reported as a standard agenda item at IGSG meetings for review.

5.6 Information Risk Assessments

In order to establish a mechanism for routinely and consistently reviewing the state of the Council's data, the Council will include Information Risk Assessments within its improvement planning and change management processes. Information Risk Assessments will assess the fitness of the Council's data for a given purpose and that there are adequate controls in place managing the data and access to it. The assessments will be applied during the introduction of new information systems or where there are significant changes to who will have access to, or process, personal data. These arrangements will be subject to testing through Council's audit and assurance regimes. Action plans arising from Information Risk Assessments will be designed to support existing corporate assurance mechanisms.

5.7 Information Asset Register

The Council maintains an Information Asset Register. The purpose of the Information Asset Register is to list the information assets within the Royal Borough, what is their function, where are they held, what type of information is stored and who has access to them. This supports the Information Governance toolkit and provides a record of all Information Assets that the Royal Borough holds, together with details on the Information Asset Owner and Administrator is held within an Information Asset Register. The Information Asset Register will be reviewed on a rolling basis against the Information Risk Assessment checklist.

5.8 Records Management policy

The Council will maintain a records management policy which sets out a corporate policy for the management of records to ensure compliance with the Local Government Act 1972, GDPR and Data Protection Act 2018 and the Freedom of Information Act 2000. The policy sets out the standards of corporate records management, including retention and corporate classification.

5.9 Information Sharing Agreements

The Council will set in place formal Information Sharing Agreements to provide a framework of trust between professionals needing to share personal information.

5.10 Business Continuity

The Council maintains Business Continuity Plans which include audits of key information systems, with an assessment of the impact of any potential disruption or interruption of those systems with appropriate controls to address these. All standard controls including backups and Disaster Recovery procedures will be in place to minimise the impact of any incident, which causes interruption, or non-availability of any information system.

5.11 Annual Health Checks

Each year the Council will assess its overall Information Governance status, organisation and documentation against best practice as defined by the Information Security Management Systems Standard ISO 27001 and against the requirements of the Health & Social Care Information Centre (HSCIC), the Information Governance Toolkit (IGT).

A health check of all Council IT infrastructure systems and facilities will be undertaken every 12 months to ensure compliance with the Public Services Network Code of Connection (PSN CoCo). This health check includes penetration testing, network analysis, vulnerability analysis and delivers a summary report with recommendations for improvement.

6 Changes, Approval and review of policies

6.1 Annual review, approval, and adoption

This policy framework and the commitment to security management is subject to continuous, systematic review and improvement. This Overarching Information Governance Security Policy Framework will be governed by the Information Governance Steering Group, which is chaired by the Information Governance Lead.

6.2 Formal approval, adoption and review

This policy will be formally signed off by the Information Governance Steering Group.