INFORMATION SECURITY POLICY

1. Overview

Information is created, stored, accessed, processed, transferred and deleted.

Hence Information Security is a wide ranging subject area covering how people behave, verifying and maintaining identities, access to computer systems, access to buildings, management of paper, how networks are managed, how software is maintained, how applications are developed, how databases are maintained, how information is managed and secured, as well as our relationships with suppliers, contracts with commissioning bodies and shared services.

The Council is obliged in the way it manages and maintains security of its information to comply with legislation such as the Data Protection Act, industry and government regulations such as:

- N3 Code of Connection
  For NHS connection and information sharing
- Government Connects Secure eXtranet (GCSX)
  For connection and information sharing with central government bodies such as DWP
- London Public Sector Network (LondonPSN)
- Payment Card Industry Data Security Standard (PCI DSS)
  This has been developed and is mandated by the card brands such as Amex, Visa and Diners Club. Essential as the Council moves more services online and hence payments are required to be transacted online rather than face-to-face

Disconnection from these services due to serious security breaches or non-compliance would severely impact our ability to efficiently deliver services to the public which often requires close working with partner organizations such as the Police, NHS, and Department of Works and Pensions (DWP).

2. Scope

This policy applies to:

- All staff at all grades and whether full time, part time, contract, permanent or TUPE’s across from other organisations

- The employees of any third party organisation who manage an information system on behalf of the Council

- All Council ICT systems such as line of business and corporate databases, intranet, internet and workstations (PCs, laptops, tablets)

This policy outlines in Policy Statements the key requirements for securing the Councils information. Where staff have specific responsibilities for information or an ICT system they will need to refer to more detailed additional policies and procedures.

3. Objectives

- To ensure staff understand their personal obligations for maintaining security
- To maintain the Confidentiality, Integrity and Availability of information and IT systems
- To ensure the risk of security breaches is minimized
- To avoid fines for security breaches and breaches of the Data Protection Act
- To run an efficient service that is able to work with partners securely to combat fraud

4. Policy Statements

1 Security Induction Training: Day 1

This is mandatory for all staff without exception and must be completed on their first day in the office. It consists of two 15 minute courses with an end of course test:

- ICT Acceptable Use
- Internet Usage

Until these courses are completed with a “pass” mark the member of staff will have limited network access (internal email and access to the Council Intranet only).

2 Security Induction Training: Month 1

This is mandatory for all staff and must be completed within their first 30 days of starting employment with the Council. There are four courses of 15 minutes with end of course test:

- Data Protection
- Information Security
- Freedom of Information
- Information Sharing

Under exceptional circumstances such as a temporary role for less than two months where information access will be limited then these Month 1 courses may be wavered.

Only a line manager can have this waver sanctioned by contacting the Councils Information Security Manager via email stating the grounds for the waver and their acceptance of the responsibility for any resulting security breaches.

3 Personal ID Badge & Building Access

Temporary badges can be issued for a maximum of 30 days for new starters. All staff must wear their ID badges prominently and challenge anyone attempting to enter Council premises without one.

4 Equipment Care & Return

You must take care of Council equipment issued to you, protecting it from damage, loss or theft following Council guidelines. Return the equipment to ICT when no longer required or when you are leaving the employment of the Council.

5 Software & System Changes

You must not make any changes to software or system settings on Council equipment of software that could undermine the secure operations of Council equipment, software or impact the network.

6 Authorised Software & Applications

You must not install or use software and applications other than that supplied or authorised for use by Council ICT. Council equipment will be supplied to you with all of the applications required to conduct your work; if it is not please inform your line manager.

7 Logon IDs & Passwords

Logon IDs (or usernames) are what identify you as unique individuals accessing Council systems.   You must never use another member of staff's computer login credentials or account profile.

You must never share or reveal your password – to do so is a serious breach of security protocols.

8 Secure Communication & Storage

The Council's email system is the only email system you will use for Council correspondence internally.

You must not set up automatic forwarding of emails to addresses external to the council. You must not copy emails to addresses outside the council unless there is a legitimate business purpose for doing so.

You must not use council email facilities for forwarding chain letters, "warning" emails, or impersonating other people.

GCSx mail accounts are provided on request for more secure external communication with public bodies (police, NHS, DWP, other Local Authorities etc).

Please contact Council ICT for other authorised secure communication methods which cover email and file transfer.

No other email or file transfer system can be used unless authorised by Council ICT.

Most free file transfer systems are not suitable as they breach the requirements of the Data Protection Act for sensitive and confidential information.

Only Council provided encrypted memory sticks can be used to store Council information.

9 Clear Desk Policy

The Council requires staff to ensure their desks are clear of paperwork at the end of the day and that these papers are then securely locked away.

As far as possible staff should reduce their reliance on paper by using online systems and digital copies and avoiding unnecessary printing particularly of sensitive or confidential information.

10 Paper & Equipment Disposal

Ensure confidential paper work is shredded and not left in wastepaper baskets or skips.

You must not dispose of Council ICT equipment yourself. Contact Council ICT for advice as secure disposal facilities are provided. This covers memory sticks, SD cards, mobile phones and scanners as well as PCs and laptops as they all potentially store data.

11 Home Working & Offsite Working

The Council's policies and guidance still apply. You will need to create an environment as close to an office environment as practical, ensuring you have somewhere secure to store equipment and confidential paperwork.

You can only use home or non Council wireless on Council equipment if the connection is via the Council's remote access gateway. Instructions for this are on the Council intranet.

12 Personal Use

You may make limited use of IT facilities for personal use, including email and web access, outside working hours (i.e. before and after work and at lunchtime).

You must not carry out any personal financial transactions (such as ordering or paying for goods or services).

You must not play internet-based games or access web-based personal email (e.g. hotmail).

Consult your manager if you need further guidance on acceptable personal use.

13 Business Activity

You must not use the council's IT facilities to conduct any private business activity.

14 Other Council Guidance

Council facilities must not be used to create, view, access or disseminate offensive, discriminatory, unlawful, obscene or other material that in the Council's view is objectionable.

You must comply with any additional Council policies or guidance issued by Council ICT.

You must ensure you read and understand any guidance and notices sent from ICTNews or Staff News email addresses as they relate to security.

15 Reporting Breaches

You must report all suspected, potential or actual security incidents and breaches as soon as you become aware of them.

You must report any accidental access to inappropriate or illegal material to your line manager.

5. Non-compliance

Non-compliance with this policy will:

- Have a serious impact on efficient operation of the Council
- Expose the Council to significant risk of substantial fines
- Increase operational costs

A breach of this policy may lead to disciplinary action being taken against you.

Any exceptions to this policy are only permitted if authorised by the Council's Information Security Manager.

Document Control

LONDON BOROUGH OF RICHMOND UPON THAMES

Reference Number	Version	Status
IG	**V1.2**	**Final**
Author(s)	**Directorate**	**Issue Date**
ICT	**ALL**	**February 2013**

Document Objectives	
To set out the acceptable use of IT in the council	
Intended Recipients	
All Staff	
Group / Persons Consulted	
IGG	
Does this document need an Equality Impact Needs Assessment?	
~~YES~~ / NO	
Approving Body	**Date Approved**
Head of ICT	
Contact for Review	**Review Date**
Information Security Manager ICT	
Approving Body Chair	
Adrian Boylan	

Version Control

Version	Date	Author	Description
1	October 2012	IT Security manager	Replaces ICT Acceptable Use Policy 2.3
1.1	February 2013	Cathy Bland	Updates from review with IGG
1.2	8/7/2014	AB	Updated links in point 7