****

**Nottingham City Council**

# Information Security Policy

|  |  |  |
| --- | --- | --- |
| **Reference** | **:** | Information Security Policy |
| **Issue No.** | **:** | 4.0.1 |
| **Issue Date** | **:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **BUSINESS APPROVAL** | |  |  |
| **Approved by** | **Position** | **Signed** | **Date** |
| **Candida Brudenell** | **Senior Information Risk Officer** |  |  |

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Status** | **Author** | **Reason for Issue** | **Date** |
| 0.1 | Draft | Liadi Balogun | Interim Policy | 10/10/2010 |
| 0.2 | Draft | Liadi Balogun | Minor amendments | 20/10/2010 |
| Final | Draft | Liadi Balogun | GCSx addition | 30/10/2010 |
| 1.1 | Draft | Laurie Ritchie | Annual Review | 09/05/2012 |
| 2.0 | Final | Laurie Ritchie | Minor updates/amendments | 13/06/2012 |
| 2.1 | Draft | Laurie Ritchie | Minor style and consistency changes, inclusion of Exception process and more emphasis on non computer based information assets. | 10/8/2012 |
| 2.2 | Draft | Laurie Ritchie | Added PCI Standards section | 29/8/2012 |
| 3.0 | Final | Laurie Ritchie | All updates above approved | 8/10/2012 |
| 3.1 | Final | Laurie Ritchie | Review and adoption of New Security Classifications | 11/03/2015 |
| 4.0 | Draft | Tim Freer | Review in line with Internal Audit recommendations | 22/06/18 |

**Distribution List**

|  |  |  |
| --- | --- | --- |
| **Copy** | **Role** | **Method of Issue** |
| 1. | All staff | Intranet |

**Notes:** 1. All roles listed above receive copies, or are notified, of updated versions of the document.

2. The Method of Issue is by access to the authorised version on the intranet.

CONTENTS

1. Introduction
2. Purpose
3. Scope and Application of the Policy
4. Breaches of Policy
5. Information Security Standards
6. Structure
7. Information Security Roles & Responsibilities
8. Legislation
9. Review

## **1 Summary**

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Nottingham City Council information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies.

This policy covers:

• Information Security Principles.

• Governance – outlining the roles and responsibilities.

• Supporting specific information security policies – Technical Security, Operational Security and Security Management.

• Compliance Requirements.

The Policy ensures business continuity and minimises business damage by preventing and diminishing the impact of security incidents. The Policy enables information to be shared, but ensures the protection of that information and related IT assets. The nominated officer for Information Security matters within the Council is The Senior Risk Information Officer(SIRO), who is ultimately responsible for identifying and mitigating security risks to the Council as a whole. The Data Protection Officer has responsibility of informing and advising The Council in relation to any data protection issues including breaches of security.

Please read this Policy and help protect our information.

## **2 Purpose**

The Purpose of the Policy is to:

* protect the Council’s information
* enable secure information sharing to deliver services
* protect the Council from legal liability and inappropriate use
* encourage consistent and professional use of information and systems
* ensure everyone is clear about their roles in using and protecting information
* maintain awareness of information security
* protect the Council’s employees
* NOT constrain reasonable use of information in support of normal business activities of the Council

This Policy is an addition other Nottingham City Council policies relating to information disclosure and personal conduct including the Data protection policy and the appropriate policy document.

## **3** **Scope and Application of the Policy**

The Policy applies to everyone who reads or processes Nottingham City Council information. The Policy applies wherever and whenever Council information is processed and applies equally to all users having access of any kind to the Council’s systems, resources and/or networks including but not restricted to:

* Councillors
* Colleagues
* All employees and agents of other organisations who directly or indirectly support or use the Council’s Information Systems including:
  + partners and suppliers,
  + contractors,
  + consultants,
  + casual, temporary or agency staff directly or indirectly employed by the Council,
  + volunteers.

The Policy applies to all forms of information, including but not restricted to text, pictures, photographs, maps, diagrams, video, audio, CCTV and music owned, administered or controlled by the Council, including information, which is:

* Spoken face to face or communicated by fixed line or mobile telephone, or by two-way radio
* Written on paper or printed out from a computer system
* Stored in structured manual filing systems which are referred to and called “relevant filing systems” in article 4 of the GDPR and Part 1 of Data Protection Act 2018, and are defined as:

*‘…any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, de-centralised or dispersed on a functional or geographical basis.’*

* Transmitted by electronic mail, fax, over the Internet and via wireless technology. (see guidance at <http://intranet.nottinghamcity.gov.uk/it-services/it-policies-and-security/secure-email-options/>)
* Stored and processed via computers, computer networks or mobile computing devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
* Stored on any type of removable computer media including, but not restricted to CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

For security purposes, all forms of information must be protected against threats such as computer based fraud, sabotage, vandalism, theft, virus attack, fire combustion and its consequences, user negligence and computer hacking.

## **4 Breaches of the Information Security Policy**

## **Definition of a breach:**

## Article 4(12) of the GDPR defines a breach as follows:

## ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’

## ***Terminology***

|  |  |
| --- | --- |
| ***Term*** | ***Meaning/Application*** |
| ***SHALL*** | ***This term is used to state a Mandatory requirement of this policy*** |
| ***SHOULD*** | ***This term is used to state a Recommended requirement of this policy*** |
| ***MAY*** | ***This term is used to state an Optional requirement*** |

Actions or neglect leading to a breach of the Policy and any of the supporting policies detailed in section 6 shall result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.

Breaches of the Policy by a user who is not a direct employee of Nottingham City Council shall result in action being taken against the user and/or their employer.

In certain circumstances the matter should be referred to the Police to consider whether criminal proceedings should be instigated.

## **5** **Information Security Standards**

The Information Security Policy and associated documentation is based on these International Standards:

* ISO/IEC 27000:2009 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
* ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements
* ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management
* ISO 22301:2012 – Business Continuity Management

## **Structure**

The Policy is divided into sections that provide a set of controls based on current security measures in use throughout the Council and supported by the IT Service, along with industry recognised security protocols.

There are a number of supporting policies that are referenced from the Policy. These are:

* IT Acceptable Use Policy
* Physical Security Policy
* IT Systems Access Control Policy
* E-Mail Policy and guidance
* Security Classifications Policy
* Social Media Policy
* IT Services Release Policy
* Data Incident and Breach Policy
* Appropriate Policy Document
* Records Management Policy
* Absent User Request Guidance
* Network Security Policy
* Wireless Security Policy
* Remote Working Policy
* Mobile Device Security PolicyException Policy
* Data Protection Policy 2018
* IT Systems Password Standards Policy
* Information Classification Policy
* Removable Media Policy

## **Information Security**

## **Principles**

## The core information security principles are to protect the following information/data asset properties:

## • Confidentiality breach – protect information/data from, unauthorised disclosures, loss of or unauthorised viewing.

## • Integrity breach – retain the integrity of the information/data by not allowing it to be modified.

## • Availability breach– maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

## In addition to the core principles, information security also relates to the protection of reputation; reputational loss can occur when any of the principles are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

## **Roles & Responsibilities**

**All colleagues shall**:

* Undertake the Information Security Training on an annual basis
* Comply with the Policy and associated security policies, processes, procedures and guidelines at all times.
* Ensure that relevant legal, statutory, regulatory and contractual obligations related to information are complied with at all times.
* Be familiar with the operation and security requirements of the information and computer systems they use in order to minimise the possibility of user error causing harm to the information’s confidentiality, integrity and availability.
* Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the Council without proper authorisation.
* Report immediately to The Data Protection Team ([data.protection@nottinghamcity.gov.uk](mailto:data.protection@nottinghamcity.gov.uk)) all suspected violations of this and all other security policies, system intrusions, and any other security incidents or weaknesses in security, which might jeopardise the Council’s information or information systems, following agreed incident management policies and processes. The data protection team will liaise with IT if immediate action is required. Guidance on reporting breaches can be found at <http://intranet.nottinghamcity.gov.uk/it-services/it-policies-and-security/report-a-security-incident/>
* Note all security notifications distributed from IT and act accordingly on advice given.
* Play an active role in protecting information in day-to-day work.

**Senior Information Risk Owner (SIRO)**

* is accountable for information risk within Nottingham City Council and advises the Board on the effectiveness of information risk management across the organisation.
* Operational responsibility shall be delegated by the SIRO to the Nottingham City Council Information Security Officer
* Promote effective and appropriate information security and risk assessment

**Data Protection Officer**

The Data Protection Officer informs and advises Nottingham City Council and its constituent business areas of its obligations pursuant to the Data Protection Legislation and provides advice in regards to all issues relating to the processing of personal data.

The Data Protection Officer shall:

* Advise on the provision of expert advice to the organisation on all matters concerning the data protection, compliance, best practice and setting and maintaining standards.
* Provide a central point of contact with the Information Commissioner’s Office.
* Communicate and promote awareness of the data protection across the council.
* Advise on matters concerning individual’s right to access information held by Nottingham City Council and the transparency agenda.
* Reports to the Corporate Management Team issues to data protection.
* Help to spread good practice in information handling.
* Assist in the development and implementation of information security policies

**Caldicott Guardian**

* Responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to our service users.

**Corporate Management Team**

* Actively promote effective and appropriate information security.
* Endorse this high level Information Security Policy and support effective and appropriate information security throughout the Council.

**All Senior Officers and Managers shall**

* Implement the Policy within their service areas and promote information security to all staff.
* Ensure that colleagues understand and abide by the Policy and its associated policies, processes, procedures and guidelines, its impact on their work and their obligations under it, in order for them to carry out their duties efficiently, effectively and securely.
* Ensure that all colleagues undertake and complete both Information Security awareness training and Data Protection Training on the commencement of employment, with refresher training being undertaken annually.
* Assign owners to all information in their area of responsibility; ensure that a risk assessment is undertaken to select appropriate security controls to protect their information; ensure that security controls continue to be effective and appropriate.
* Ensure that all staff report personal data security breaches to The Data Protection Team and IT Security (none personal)
* Apply security controls relating to colleagues and ensure that job descriptions address all relevant security responsibilities.
* Provide written authorisation for access to information.
* Ensure that communications regarding information security are cascaded effectively to all colleagues.
* Ensure that information security is an integral part of all services’ processes.
* Ensure that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures

**Information Asset Owners shall**

* Working with relevant responsible officers select the security controls required to protect their information appropriately.
* Monitor to ensure security controls continue to be effective and that information is being handled correctly.
* Report and act on security incidents and weaknesses relating to their information according to agreed incident management policies and processes.
* Ensure that the Information Asset Register (<http://ims.nottinghamcity.gov.uk/iar> is updated and that the data mapping exercise carried out and any risks identified are mitigated.
* Have in place appropriate Business Continuity plans and contingency arrangements.
* Have awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
* support personal accountability of users within the business area(s) for Information Security

**Nottingham City Council IT Security**

* IT Security is the responsibility of all colleagues in the Council, but especially those in the IT Service who are responsible for ensuring it is taken into account throughout products and services’ lifecycles.
* The Head of the IT Service provides advice on IT Security matters to the SIRO through the Information Management Advisory Board.
* The IT Service is responsible for
  + ensuring the Council’s compliance with directed IT security related standards including PSN compliance
  + monitoring potential and actual security breaches with appropriate expert security resource.
  + ensuring the operational effectiveness of security controls and processes.
  + ensuring that all appropriate security patches are distributed and installed across the estate in a timely fashion
  + ensuring that software version upgrades are reviewed/implemented regularly where required to ensure continued security compliance

**Legislation**

Nottingham City Council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Council, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Council shall comply with all relevant legislation appropriate; this includes but is not limited to:

* + Common law in relation to duties of confidentiality
  + Health and Safety at Work Act 1974
  + Theft Act 1978
  + Indecent Display (Control) Act 1981
  + Obscene Publications Act 1984
  + Copyright, Designs and Patents Act 1988
  + Computer Misuse Act 1990
  + General Data Protection Regulation (GDPR) 2016/679
  + Human Rights Act 1998
  + Protection of Children Act 1999
  + Freedom of Information Act 2000
  + Regulation of Investigatory Powers Act 2000
  + Terrorism Act 2000
  + Data Protection Act 2018
  + Privacy and Electronic Communications Regulation 2003

**Review**

This policy shall be reviewed at least annually at the discretion of the SIRO