North Yorkshire Fire & Rescue Service

Information Security and Handling Policy

Table of Contents

1. Introduction.....4

2. Purpose.....4

3. Scope..... 4

4. Policy..... 4

5. Policy Governance.....7

Document Change History

Date	Version	Status	Author	Details of Change
02.06.2010	0.1	Draft	Head of ITSS	Initial Document
02.02.2012	1.0	Final	Head of Service Development	Review and format change
02.02.2012	2.0	Final	Head of Service Development	Title change
18.09.2014	3.0	Final	Head of ITSS	Update links to ICT policies
15.6.2015	4.0	Final	CAO Manager	Included DBS statement

This is an electronic version of the approved version and paper copies are only valid as of the last update. Please refer to the master copy or the document author if you are in any doubt about the document content.

Policy Superseding:

This policy supersedes the following policies from the date adopted date in the information panel:

- Information Handling Policy – Draft
- Information Security Policy - Draft

Contributors:

Development of this policy was assisted through information provided by the following organisations:

- Information Commissioners Office website

1 INTRODUCTION

This policy provides an overarching framework for information security controls across the Authority and is based on the ISO27001:2005 standard.

2 PURPOSE

The policy aims to ensure that North Yorkshire Fire and Rescue Service's information assets and resources, both technological and not, are appropriately protected.

3 SCOPE

This policy applies to staff, contractors, consultants, temporaries, and other workers at North Yorkshire Fire & Rescue Service including all personnel affiliated with third parties.

This policy applies to all information. This includes information in the following forms:

- Printed
- Written or Paper
- Stored electronically
- Transmitted by post or electronic means
- Shown on films
- Recorded speech or images
- Spoken in conversation

Where this policy contains reference to sensitive information this refers to information that is:

- Personal in nature
- Commercially sensitive
- Could compromise security
- Could be involved in legal proceedings
- Management information for later publication

A more detailed consideration of sensitive and personal information is contained in the 'Intranet Secure Site Register SOP'.

4 POLICY

4.1 STAFF

4.1.1 Human Resources will perform adequate security screening prior to employment of permanent or temporary staff. The screening will be dependant on the role but as a minimum references will be sought and identity will be checked in accordance with Right to Work in UK legislation.

4.1.2 The Equality and Safeguarding Officer will use the Disclosure and Barring Service (DBS) to assess the suitability of applicants for identified positions of trust, such as Community Safety Officer, LIFE, BTEC, Crucial Crew instructors and Firesetter case workers, who will all be subject to an enhanced disclosure. The Service complies fully with the DBS Code of Practice and Data Protection Act 1998 requirements

regarding the correct handling, use, storage, retention and disposal of Certificate information.

4.1.3 Staff Written Statement of Particulars will detail the necessary terms and conditions that are appropriate for their role.

4.1.4 All staff must read this policy and in particular the;

- ICT - Usage Policy

- Staff Code of Conduct
- Data Protection Policy
- Visual Imaging Policy
- Social Media Policy

Individuals are responsible for familiarising themselves with the necessary policies that are appropriate for their role.

4.1.5 Appropriate information security and handling training must be completed by all managers and specialist staff. Identified staff will also attend any necessary Data Protection courses.

4.1.6 All employees are required to complete the Protecting Information Learn Pro module and Social Media Learn Pro module every 2 years,

Module	Applicable to
Protecting Information – Level 1	Non Rider, Control and Non Uniformed staff
Protecting Information	Watch and RDS staff
Social Media	All employees

4.1.7 Regular reminders will be issued to all staff emphasising the importance of information handling and security along with any updates or changes to policy, e.g. via information bulletins or special staff newsletters when required.

4.1.8 All information resource users, including system administrators are uniquely identified on each system accessed. All users are authenticated using a password which must be assigning in accordance with the ICT - Security Policy.

4.1.9 Access to systems and information is on a restricted need to know basis and requires approval from the system or information asset owner.

4.1.10 Staff must exercise caution to prevent unauthorised persons from viewing North Yorkshire Fire and Rescue Service's confidential or sensitive information.

4.1.11 There is a Leavers Process SOP to ensure protection of information when an employee leaves the Service.

4.2 PHYSICAL SECURITY

4.2.1 All staff are responsible for protecting North Yorkshire Fire & Rescue Service's information assets, staff, property, services, revenues, proprietary information and image from damage, theft, misuse, or unauthorised use.

4.2.2 Only Service staff or authorised agents are allowed unescorted access to Service facilities except where specific facilities exist such as community rooms. All premises have a minimum level of security ranging from door locks to alarms and keypad access depending on the level of security required.

4.2.3 Critical business information processing facilities are housed in secure areas and have the necessary protection based on the risk of the information / asset being compromised or destroyed.

4.2.4 Unsupervised work activity in secure areas is to be avoided both for personnel safety and to prevent opportunities for malicious actions.

4.2.5 Assets, including buildings and vehicles, should be secured at all times when left unattended. Small items should be securely stored away and/or password protected. See the suite of ICT policies relevant to the specific IT equipment.

4.3 EQUIPMENT USE

4.3.1 Equipment, including personal computing devices and portable or handheld devices must be physically protected from security threats, environmental hazards, and maintained according to manufacturer's specifications. Reference should be made to the ICT – Assets Policy, ICT - Security Policy and the ICT – Usage Policy.

4.3.2 Computers, storage components, removable storage media, and printed products that contain or have ever contained North Yorkshire Fire & Rescue Service information must be disposed of in a secure manner, and in accordance with published policies, e.g. Disposal of IT equipment will be in accordance with the ICT – Assets Policy

4.3.3 Contractors are required to verify the use of an anti-virus software product with current downloaded signatures on their systems before accessing North Yorkshire Fire & Rescue Service's network if a North Yorkshire Fire & Rescue Service provided secure system is unavailable.

4.3.4 All computing assets, including mobile devices will be password protected. Staff should refer to the ICT - Security Policy.

4.3.5 All new systems and / or enhancements to existing systems must have a risk analysis and a vulnerability scan performed to identify areas of vulnerability, and to ensure those areas are properly addressed prior to production re-deployment. The risk analysis will consider whether the new system or enhancement will impact on existing applications. Consideration will be given to completion of a Privacy Impact Assessment.

4.3.6 Development and testing of new / existing IT equipment must be performed in an environment that is separate from any live system

4.3.7 All IT staff and contractors must make themselves familiar with the IT suite of policies relating to IT equipment.

4.4 INFORMATION MANAGEMENT

4.4.1 The Service has a Protective Security Marking Policy and Information Handling Procedure that must be adhered to for the management of information. All staff must make themselves familiar with these documents.

4.4.2 Printed and written documentation that contains sensitive information must be kept in locked cabinets or drawers. Access to the keys must only be given to staff that have permission to access that information. Information must be deleted in line with the Retention Schedule and should be disposed of securely either by shredding or putting into a confidential waste sack (which should be kept in a locked cabinet).

4.4.3 Electronic documents or data that contain sensitive information should be saved in a secure area of the Intranet whereby permissions are set only to those who are permitted access to the information. It must be on a business 'need to know basis.' The Intranet Secure Site Register Procedure provides guidance on whether the site or library needs to be on the secure site register. Electronic Information must be deleted in line with the retention schedule.

4.4.4 Staff should ensure that all sensitive information, either in paper or electronic formats, are not on view to casual observers or visitors when in use. Staff should lock their computer screens when away from their desk to prevent unauthorised access. Printed documentation containing confidential or personal information should be removed from printers and faxes.

4.4.5 Staff should not remove information from a place of work unless it is necessary to do so. Staff should ensure that they take adequate measures to protect the service's information.

4.4.6 Staff should take care when e-mailing documents to internal or external recipients. If the email contains sensitive information, seek clarification from your manager on whether it is acceptable for the information to be released.

4.5 INFORMATION SECURITY BREACH

4.5.1 A security breach may arise from a theft, a deliberate attack on systems (internal or external), the unauthorised use of personal data or unauthorised access to sensitive data by a member of staff or from accidental loss or equipment failure.

4.5.2 Any member of staff who becomes aware of a security breach must inform the Central Administration Office (CAO) or ITSS. Out of hours the senior officer should be informed via Control.

4.5.3 The Information Governance Group will manage the response to the breach and if it is serious enough a business continuity management team will be set up. The aim of this response will be to the secure the systems and recover the information and then to investigate the cause to prevent re-occurrence.

5 POLICY GOVERNANCE

Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
  N.B Only **one** role is held accountable.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Information Governance Group
Accountable	Director of Finance and Service Development
Consulted	ITSS, CAO
Informed	All staff, all temporary Staff, all contractors etc.