| | |
|---|---|
| PS | Information Security |
| Type of Document | Policy |
| Version | 1.0 |
| Registered Owner | Kevin Dennis |
| Author | Karen Sleigh |
| Effective Date | 1st September 2014 |
| Review Date | |
| Replaces Documents | |
| Linked Documents | Risk Management<br>Records Retention and Disposal<br>Data Protection |

**Table of Contents**



## 1.0 Section 1 Version Control

| Version No | Date | Post Holder Author | Post | Reason for issue |
|---|---|---|---|---|
| 1.0 | August 2014 | Karen Sleigh | | New policy |

## 2.0 Section 2 Background

2.1 The Office of the Nottinghamshire Police and Crime Commissioner is wholly committed to setting the highest standards of delivery in Information Security.

2.2 The Information Security policy represents a high level position for Office of the Nottinghamshire Police and Crime Commissioners in the Protection of physical assets listed as:

- CCTV:
- Buildings Security:
- Individuals (ID Card & Vetting):
- Accessing Computer terminals and Network Security Access
- Email and text:
- Mobile Devices:
- Staff Training:
- Clean / Clear Desk policy:

Implementation of this policy will address all threats whether internal or external of the Office of the Nottinghamshire Police and Crime Commissioner.

2.3 This policy is the master policy and must be reflected in all other policies, read in conjunction with Risk Management and Records Retention and Disposal Policies.

2.4 All individuals 'working' for the Office of the Nottinghamshire Police and Crime Commissioners are required to read and comply with the requirements of this policy at all times.

## 3.0 Section 3 Aims / Objectives

3.1 It is the Office of the Nottinghamshire Police and Crime Commissioner's aim to create an environment whereby all data held is:

- Accurate
- Adequate
- Relevant
- Timely

3.2 All business processes must ensure staff awareness of a:

- Consistent professional approach:
- Clear as to their role:
- Their individual security:
- Use of information including encryption:
- Ensure business continuity (data back-up):
- Proactive identification of potential security breaches and reporting:
- Entries in the risk and data protection registers where appropriate:

Staff will use all lawful means at their disposal to protect data and the Office of the Nottinghamshire Police and Crime Commissioners from legal liability and inappropriate use of information.

3.3 All mobile devices (mobile phone or laptop) used by staff must be owned and issued by, or where commissioned to deliver a service, on behalf of the Office of the Nottinghamshire Police and Crime Commissioners only.

3.4 A register of the devices and to whom they were issued will be held by the Office of the Nottinghamshire Police and Crime Commissioners. This will include:-

- Make;
- Model;
- Serial Number and
- Telephone Number
- Device issued to

3.5 All mobile devices must be password protected at two levels: accessing the device and accessing a file.

3.6 Any loss of a device must be immediately reported to Office of the Nottinghamshire Police and Crime Commissioners and entered on the Data Protection Register including the completion of a risk assessment as to impact of loss.

3.7 Office of the Nottinghamshire Police and Crime Commissioners does not permit the use of BYOD (bring your own device) within the work environment.

3.8 A decision to notify the Information Commissioners Office may be required by the Chief Executive, in the event of data loss. This will include notifying any victims of the data loss and impact on the victim's life.

## 4.0 Section 4 Details

### 4.1 Application

All staff are required to ensure they have read and understand the Office of the Nottinghamshire Police and Crime Commissioners Information Security policy. They are required to sign a record accepting the policy to be held in their HR file.

The policy must also be read and agreed by all temporary employees: contracted businesses or staff working for Office of the Nottinghamshire Police and Crime Commissioners. Copy of the policy will be subject of a signature accepting the policy, held by HR Office of the Nottinghamshire Police and Crime Commissioners in line with Data Retention policy.

### 4.2 Key Principles

4.2.1 **Protection of physical assets buildings** will be access controlled: - using CCTV. CCTV images are held for 7 days only on the CCTV server with reduced access to nominated individuals within the Office of the Nottinghamshire Police and Crime Commissioners.

4.2.2 **Door access** is controlled by an ID card and secured number access to the premises.

4.2.3 **Individuals** will be subject to the Police vetting process before accessing any systems whether full; part time or as contracted staff or will be accompanied by staff whilst on premises at all times.

Each individual will be issued with either:-

- A full ID card containing:
- Their picture;
- Name or
- Hold a visitor's security pass in order to access and egress buildings safely in the event of a health and safety incident.

4.2.4 **ID card access** - This requires the user to hold the card close to the security point to open doors.

Staff will ensure ID cards are worn at all times when on the Office of the Nottinghamshire Police and Crime Commissioners premises or premises commissioned to deliver a service on behalf of the Office of the Nottinghamshire Police and Crime Commissioners. Staff failing to wear a pass will be subject to "check and challenge" at any time by members of staff.

Staff **will** ensure all doors are securely closed behind them on entering and leaving the premises.

Visitor access is strictly controlled and requires a signature on visitors register with entry provided not just for security but in compliance with health and safety in the event of fire in the building.

4.2.5 **Protection of Physical assets – Accessing Computers:** Office of the Nottinghamshire Police and Crime Commissioners applies a 90 day password protection access rule.

After this period passwords will have to be changed in line with the adopted convention (Microsoft). Data will be held on computers in line with HM Government guidelines on governance at Information Level 3 or greater at all times.

Computers desktop or mobile will be subject to Anti-Virus (AV) protection with the responsibility held by IT Department.

Desktop computers and laptops must be subject to screen lock where the user is away from their terminal. The system will lock the user out within 2 minutes of inactivity requiring password to regain access.

4.2.6 **Inbound access to software** – No download of software will be permitted unless approved by Office of the Nottinghamshire Police and Crime Commissioners with a business case for use.

Downloading of case files using approved software (word excel as examples) will be via USB iron key only, password protected and all files will be scanned using Anti Virus before acceptance onto Office of the Nottinghamshire Police and Crime Commissioners systems.

4.2.7 **Outbound access** – limited to "read only" by default on DVD: USB stick or email to include syncing of mobile devices owned by Office of the Nottinghamshire Police and Crime Commissioners.

Where the data is held on a mobile device the device must be password protected as well as the data.

4.2.8 **Email**- Office of the Nottinghamshire Police and Crime Commissioners owns all email and the subject box will have a default state of Restricted. This can be amended to Unrestricted: or specifically marked as "Personal" in the subject box if required.

Where emails are required due to an investigation authority at Executive level will be required to enter an individual's email facility. Emails are stored despite deletion in line with MOPI.

4.2.9 **Staff training** – Responsibility of HR or Training induction entry, with annual reminders, as well as ongoing reminders throughout the year will ensure Information Security and Data Protection remains at the forefront of Office of the Nottinghamshire Police and Crime Commissioners culture.

4.2.10 **Clean / Clear Desk policy** – will be adhered to supporting client data confidentiality. The aim will be "clear desk" at the end of each work day.

## 5.0 Section 5 Legislative and Compliance

5.1 This document has been drafted to comply with the general and specific duties governed by the European Convention on Human Rights; EU Regulations on Data Protection and Data Protection Act 1998 and the ACPO Guidance on the Management of Police Information (MOPI) 2010.

5.2 This document will be subject to an annual audit review to support compliance and review process