OFFICIAL

Published | | Event History

Policy owned by DCC Directorate
FiSP - Force Information Security Policy

1. Policy Purpose and key drivers

The aim of the policy

The Force Information Security Policy has been produced to provide baseline security requirements in order to safeguard the confidentiality, integrity and availability of all information held by Staffordshire Police. The purpose of this policy is not to obstruct but enable the information sharing processes of Staffordshire Police. All personnel with access to information owned by Staffordshire Police will be made aware of and required to comply with the provisions of the policy .

The policy sets out to implement the requirements of the National Policing Community Security Policy together with the business and operational demands of Staffordshire Police.

The principles and scope of the policy

The Force Information Security Policy applies to all manual and electronic information processes owned by Staffordshire Police. The policy provides a common basis for the Force to develop, implement and measure effective information security management practice.

The policy applies to all Police Officers, Police Staff, Partnership Staff and all personnel contracted to work for Staffordshire Police, Special Constables, Volunteers, temporary personnel and trusted employees from agencies and organisations who by the nature of their role require access to Staffordshire Police information systems.

This policy is written in compliance with the National Policing Community Security Policy, HMG's Security Policy Framework (SPF) and ISO/IEC 27001:2013: Information Security Management Systems – Requirements. These include the following:

- Security policies
- The security structure
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operational security
- Communications security
- Systems acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management
- Compliance checking

The origins/background information

Staffordshire Police is dependent upon information, and consequently on the systems upon which information is processed. This policy sets out the strategic aims and objectives of the Force in relation to information protection for manual, electronic and mechanical systems.

Due to the current dependence of almost all organisations upon information communications technology (ICT), as might be expected, the content of this document includes many references to ICT information systems. The security of manually held information is, however, equally important and, where appropriate, is covered in some detail in the relevant areas of the policy framework.

The general public has a right to expect that all members of the Force will, when utilising information in connection with Force business, ensure its confidentiality and integrity (particularly in relation to personal information) and availability. It is important that the right information is made available to those who need to use it for either operational or administrative purposes. When considering the availability of information employees should understand the benefits of making information available to those who 'need to know' and therefore should follow relevant guidance when supplying information.

The loss, damage, wrongful destruction or wrongful disclosure of information could result in substantial costs to the Force as well as public embarrassment and a reduction in public confidence.

Motivators/Driving Forces

The National Policing Community Security Policy (CSP) and Security Policy Framework (SPF) are intended to provide a common basis for the 'policing community' to develop, implement and measure effective security management practice and to provide confidence in inter-community dealings and third party access/supply.

General Principles of the Policy

The key area of this policy ensures that Staffordshire Police, in common with the rest of the Police Service, acts appropriately in order to maintain the confidentiality, integrity and availability of the information that it holds. This applies to its own information or that with which it has been entrusted by other organisations.

The procedures developed to support this policy will be published separately and will contain appropriate guidance to staff. It is the responsibility of all staff to ensure that they are familiar with and adhere to these procedures.

It is the responsibility of each employee to adhere to this Policy and to:

- Comply with general security instructions,
- Comply with the force Generic Security Operating Procedures.
- Report any security incidents in accordance with agreed procedures.

- Advise line managers and the Information Security Officer, as appropriate, of any potential weaknesses in information security or associated procedures

Related Documents	
Links to related documents:	FiSP - Auditing and Protective Monitoring (Procedure) FiSP - Computer Access Control (Procedure) FiSP - IT access for Non Staffordshire Police Employees (Procedure) FiSP - Password (Procedure) FiSP - Physical Access Control (Procedure) FiSP - Physical Security (Procedure) FiSP - Removable Media Devices (Procedure) FiSP - Security Incident Reporting and Response (Procedure) FiSP - System Back-Up (Procedure)
Gatekeeper - the Author suggested the following Procedure document(s) to link to.	

Relevant Dates and Review Period	
Effective Date:	01/10/2009
Review Date:	01/02/2021
Review Frequency:	Annually

Policy Basis and Implications	
2. Legal Basis:	-
3. Management of Police Information (MoPI):	MoPI Policing Purpose: Any duty or responsibility arising from common or statute law MoPI Review, Retention and Disposal addressed as follows: Not Applicable
4. Associated Benefits:	It will ensure that Staffordshire Police is able to process information securely and is compliant with relevant legisation, helping not to bring any financial penalties on itself from the Information Commisioners' Office.
5. Consultation:	Office Police and Crime Commisioner Unison Police Federation Head of Corporate Communications Head of Information Assurance Team Information Security Manager Review and Archive Unit Manager Head of Corporate Services Head of Crime Administration Unit Head of People Services Head of Business Services Benefits Realisation Team Head of Technology Services Systems Security Team Leader Head of Peoples Performance Assessment Unit Chief Inspector Local Policing Chief Inspector PVP Contact Service Manager Force Crime Registrar Senior Information Risk Owner (DCC)
6. Financial Implications:	The aim of this policy is to ensure that the Force efficiently and effectively manages the risks to its information systems and the information they hold, whilst providing appropriate security at a proportionate cost. This will result in a requirement to manage residual risks.
7. Human Resources /	No additional staffing is necessary for the implementation of this policy.

Training:	However, there is with a mandatory requirement for all members of staff to complete the NCALT Managing Information. All new starters will have to complete this course as part of their induction.
8. Associated Policy:	National Policing Community Security Policy Security Policy Framework (SPF) HMG Information Security Standards ISO/27001 Manual of Guidance 2006 Management of Police Information (MoPI) Government Protective Marking Scheme (GPMS) Policy Vetting Data Protection; Force Information Security Handbook; Information Management Strategy (IMS);

FOI, Human Rights and Equality Impact Assessment Indicators

FOIA:	Release to Public		
ECHR:	Compliant with proportionality test	Articles engaged:	Article 5 Right to Liberty and Security; Article 8 Right to respect for Private and Family life; Protocol, Article 1 - Protection of Property
EIA:	Compliant	Compliant with Code of Ethics:	Yes

Indexing

Categories:	Information Management

OFFICIAL