

WILTSHIRE POLICE & POLICE AND CRIME COMMISSIONER



Information Security Policy

Date of Publication: May 2021
Version: 4.0
Next Review Date: May 2023

TABLE OF CONTENTS

TERMS AND DEFINITIONS.....	3
POLICY STATEMENT	4
SCOPE	5
ROLES AND RESPONSIBILITIES	5
ACCREDITATION	6
MOBILE & REMOTE WORKING.....	7
THIRD PARTY & SUPPLIER REMOTE ACCESS.....	7
INCIDENT REPORTING	7
NEED TO KNOW.....	7
PHYSICAL SECURITY	8
SECURITY EDUCATION AWARENESS & TRAINING	8
PRACTICE DIRECTIONS	8
POLICY AIM	8
APPLICABILITY	8
LEGAL BASIS AND DRIVING FORCE	8
RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS	8
AUTHORISED PROFESSIONAL PRACTICE.....	9
DATA PROTECTION	9
FREEDOM OF INFORMATION ACT 2000	9
MONITORING AND REVIEW	9
WHO TO CONTACT ABOUT THIS POLICY	9
 DOCUMENT ADMINISTRATION.....	 10

TERMS AND DEFINITIONS

Accreditation

The process to ensure that the security policy has been implemented to reduce risk for an IT system to an acceptable level.

Asset

Anything that has value to the organisation.

Availability

The property of being accessible and usable upon demand by an authorised entity

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Information Security

Preservation of Confidentiality, Integrity and Availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

Information Security Event

An identified occurrence of a system, service, network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Information Security Incident

A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Integrity

The property of safeguarding the accuracy and completeness of assets.

Risk Management

Coordinated activities to direct and control an organisation with regard to risk.

POLICY STATEMENT

Safeguarding the confidentiality, integrity and availability of all information and associated assets held by Wiltshire Police and the OPCC is paramount to ensuring public confidence in the delivery of public services and therefore supports the strategic goals of the Force. Consequently Wiltshire Police (the Force) and the OPCC must manage business impacts and risks of all information and associated assets.

The Force and OPCC recognise the importance of all information assets and the need for proper, effective management of all information processes. It is essential therefore that there are safeguards and counter measures in place to provide the continued confidentiality, integrity and availability of Force and OPCC information. Furthermore, the Force and the OPCC have a requirement to comply with relevant regulatory and legislative requirements and to be able to demonstrate this.

The achievement of information security needs a combination of policies, standards, procedures, guidelines, appropriate organisational structure, physical security considerations, and measures to safeguard the IT network infrastructure and information systems.

This policy provides an overarching structure for information security throughout the Force and OPCC. This Policy forms the structure for practice directions and other security procedures relevant to information security.

All personnel with access to information owned by the Force and/or OPCC will be made aware of, and, are required to comply with the provision of this Policy.

Wiltshire Police and OPCC recognise the need to ensure information and information assets are managed and protected appropriately. The Policy aims to support this by providing a 'defence in depth' approach that encompasses four main areas:

- Physical Security;
- Personnel Security;
- Technical Security;
- Policies and Procedures.

Fostering a professional culture and developing a positive attitude toward security is critical to the successful delivery of this Policy and in support of this the Force and OPCC will ensure that those responsible for information security and management are made aware of their responsibilities.

In support of this policy, the Force and the OPCC will:

- Ensure that information is accessible only to those authorised to have access;
- Ensure the Force/OPCC IT systems, applications and networks facilitate the security of our data;
- Safeguard the accuracy and completeness of information and processing methods;
- Ensure that we meet our regulatory, legislative and contractual requirements;
- Address the security of all of our services and processes to ensure that risks are identified and appropriate controls are implemented and documented;
- Provide a secure working environment for staff and contractors at our premises;
- Produce incident response plans for essential Force functions, supporting services and infrastructure, which will be maintained and tested on a regular basis;
- Require all third parties working on our behalf to ensure that the confidentiality, integrity and availability requirements of all business systems are met;
- Promote security awareness and provide appropriate information security training for our employees.

SCOPE

The Policy applies to all information (including information processes) and assets owned by the Force and OPCC. The Policy provides a common basis for the Force/OPCC to develop, implement and measure effective information security management practices.

The Policy and associated practice directions apply to all Police Officers, Police and OPCC Staff, Special Constables, Volunteers and employees from agencies or organisations who by the nature of their role, are required to access Force/OPCC information and information assets.

ROLES AND RESPONSIBILITIES

Information Security Governance Board (ISGB)

The IGSB, Chaired by Deputy chief Constable (SIRO), has ownership of the Force Information Security Policy.

The IGSB is the governance authority responsible for commissioning and approving all activities, policies, standards and guidelines relating to the Information and Security landscape.

The objective of the board is to provide strategic direction and oversight for both Wiltshire Police and Wiltshire OPCC on matters relating to information governance and security and to provide guidance for each Senior Information Risk Owner (SIRO) to fulfil their statutory roles on behalf of their organisation.

ISGB will:

- Meet as quarterly. Additional meetings may be scheduled by the SIRO where required.
- Provide effective and consistent governance to ensure that information is treated as a strategic asset and managed as such
- Direct the development of more effective information processes and policy across the force and with partner agencies
- Create a consistent and measurable approach to the development of information capability and formally report progress as agreed by the SIRO to ELT and CMB
- Ensure that there are the minimum set of Systems, Applications and Standards to manage and exploit information effectively across Operational, Enabling Service and OPCC areas of business

Senior Information Risk Owner (SIRO)

Deputy Chief Constable is responsible for establishing a comprehensive programme of work to achieve progress through identifiable milestones, ensuring information risk management is embedded organisationally, best practice IA measures are implemented and effective legislative / regulatory body compliance expectations regarding the management of information and business risks, as they relate to policing priorities, are achieved and maintained.

Head of Information Management and Assurance

The Head of Information Management and Assurance is responsible for establishing an information risk and security management system proportionate to Force size, structure, policing priorities, strategies, plans & objectives, security requirements and implemented processes. Operational responsibilities are detailed in the Information Risk Management Policy.

Records Manager

The Records Manager is responsible for maintaining an information asset register, recording all Wiltshire Police 'critical information assets' in conjunction with a range of information relevant to managing risk to each asset and ensuring compliance with Authorised Professional Practice and Statutory Guidance on the Management of Police Information (MoPI) requirements and expectations.

Information Asset Owners (IAO)

IAO are required to understand what information is held, what is added and what is removed from Information Systems (IS) under their control, who has access and why. Consequently, they will be able to understand and address risks to the information over which they have responsibility and ensure that information is fully used within the law for public good. IAO will not assume ownership of any corporate risks that are incurred outside the scope of their particular area of responsibility including projects and or programmes.

Commanders and Heads of Department

Commanders and Heads of Department (Force and OPCC) are responsible for the day to day security and management of all information processes within their area of responsibility and are required to ensure local compliance with this and other security policies, procedures and processes.

Information Security Officer

The Information Security Officer is responsible for coordinating and implementing technical aspects of Information Security effectively across the Force and the provision of technical support to the Head of Head of Information Management and Assurance.

Force Data Protection Officer (DPO)

Data Protection Officer is responsible for providing 'Notification' to the Information Commissioner of all processing of personal data by Wiltshire Police and OPCC, ensuring processing is fully compliant with the requirements of the DPA 2018 and General Data Protection Regulations and supporting the Accreditation process by considering the requirement for Privacy Impact assessments (PIA) to be undertaken.

Line managers

Line Managers are responsible for ensuring compliance with the Policy and Practice Directions by the regular monitoring of their staff and information processes.

Users

All personnel have a personally assigned responsibility for the preservation of the confidentiality, integrity and availability of information systems accessible by them and information entrusted to them. Information can only be used for permitted policing purposes. Specific responsibilities and accountabilities are detailed in Security Operating Procedures (SyOPs).

ACCREDITATION

All information systems, services and applications processing, handling or storing protectively marked or other sensitive information will be subject to a process of security accreditation in accordance with HMG Information Assurance Standards and accreditation / security requirements will be specified in all IST contracts.

Security Operating Procedures (SyOPs)

SyOPs, designed to assist in the efficient operation of IS detail the security standard against which all IS will be operated, define roles and responsibilities and notify users what they can and cannot do. They include:

- Scope
- System Management
- Physical & Environmental Security
- Communications & Operations Management

-
- System Administration
 - Starting up and Ending Sessions
 - Identification & Authentication
 - Counter Compromise Action
 - Incident Reporting & Management
 - Information Exchange
 - Protective Monitoring / Audit & Accounting

All Users of Information Systems are required to comply with SyOPs at all times and non compliance can result in misconduct or in some case criminal proceedings being instigated.

MOBILE & REMOTE WORKING

The Mobile and Remote Working Policy will detail the security, supervisory, routine usage, health & safety, legal and limitation on use requirements of the Wiltshire Police.

THIRD PARTY & SUPPLIER REMOTE ACCESS

The Third Party / Supplier Remote Access Policy sets out the conditions that are required to maintain the confidentiality, integrity and availability of Wiltshire Police and OPCC information and information systems when third parties require access. No Third party access is allowed until the appropriate Head of Technical Service agrees and provides written permission.

INCIDENT REPORTING

Accurate and timely reporting of security incidents is vital to reducing the potential impact and damage to the Force/OPCC. All security incidents are to be reported to the ICT Service Desk as soon as it is practicable to do so.

Incidents (as defined in SyOPs) will be recorded for onward reporting to PolWARP in accordance with Procedures for Use of the Police Warning, Advice and Reporting Point (PolWARP). The reporting format will be dictated by the type of incident and is divided into two categories – Fast Time Incidents and Slow Time Incidents. Incidents involving cryptographic items will be reported to CINRAS and will be handled according to the national Policy for Handling Cryptographic Incidents reported via CINRAS.

Some security alerts could originate from the National Monitoring Centre (NMC), these will be managed similarly within the force with national oversight by NMC.

NEED TO KNOW

The effective use (including the sharing) of information is a key priority for the Force and OPCC.

Access to information and supporting processes is required for the efficient conduct and management of operations but will be limited to those with a demonstrable need to know and use it who have been appropriately security cleared. In all cases, access to information will be on a least privilege basis. Information and other assets, including supporting processes will be managed and safeguarded to documented levels throughout their lifecycle, including creation, storage, transmission and disposal.

Asset Classification & Control

The Force and OPCC has adopted the Government Security Classification Scheme

Protecting Personal Data

Personal data will be protected from unauthorised access, disclosure, release and loss, and will be handled in accordance with prevailing legislative requirements and specific minimum measures covering access, removable media, controlled disposal, authentication and audit and those with access to or management responsibility for personal data will undergo appropriate training. Information Sharing Agreements (ISA) will explicitly address security requirements.

PHYSICAL SECURITY

People, information, infrastructure and equipment assets will be afforded physical protection commensurate with the threat, the impact / consequence of loss / compromise, vulnerability, value and local circumstances / environment. The layered / defence in depth approach incorporating prevention, detection, response and recovery is detailed in the Physical Security Policy. Headline expectations (clear desk, security furniture, clear screen, start cease work checks etc) are addressed in SyOPs.

SECURITY EDUCATION AWARENESS & TRAINING

All personnel will receive appropriate instruction with regard to information security and will be required to re-affirm compliance with the Policy at regular intervals. Additionally, all personnel are required to ensure they remain current with 'Practice Directions' published for reference on the Intranet / SharePoint.

PRACTICE DIRECTIONS

Practice Directions provide personnel with guidance on specific subjects and should be read in conjunction both with this Policy and, where appropriate, the relevant SyOPs

POLICY AIM

This Policy applies to all information (including information processes) and assets owned by the Force and the OPCC. The Policy provides a common basis for the Force and OPCC to develop, implement and measure effective information security management practices.

APPLICABILITY

This Policy applies to all Police Officers, Police and OPCC Staff, Special Constables, Volunteers and employees from agencies or organisations who by the nature of their role, are required to access Force and OPCC information and information assets.

LEGAL BASIS AND DRIVING FORCE

BS ISO/IEC 27001:2005 BS 7799-2:2005
Human Rights Act 1998
Computer Misuse Act 1990
Data Protection Act 2018
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Official Secrets Act 1989

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

Acceptable Use of Force Systems Policy
Information Risk Management Policy
Mobile and Remote Working Policy
Physical Security Policy

AUTHORISED PROFESSIONAL PRACTICE

[Information Management > Information Assurance](#)

DATA PROTECTION

Any information relating to an identified or identifiable living individual recorded as a consequence of this policy will be processed in accordance with the Data Protection Act 2018, General Data Protection Regulations and the [Force Data Protection Policy](#).

FREEDOM OF INFORMATION ACT 2000

This document has been assessed as suitable for public release.

MONITORING AND REVIEW

This Policy will be reviewed bi-annually by the Head of Information and Assurance, and at other times as dictated by organisational needs.

WHO TO CONTACT ABOUT THIS POLICY

The Head of Information Management and Assurance is responsible for this policy. All queries relating to this policy should be directed to the Force Information Security Officer or Force Policy Officer.

DOCUMENT ADMINISTRATION

Ownership:

Department Responsible: Information Management and Assurance
Policy Owner/Author: Head of Information and Assurance
Technical Author: NCC Group
Senior Officer/Manager Sponsor: Deputy Chief Constable

Revision History:

Revision Date	Version	Summary of Changes
05.06.2017	3.0	Non Substantive Change & Bi-annual Review. – Authorisation: SIRO
25.05.2018	3.0	Data Protection section amended to reflect implementation of GDPR & new DPA.
12.05.2021	4.0	Scheduled review. Minor amendments to job and board titles; policy extended to cover OPCC.

Approvals:

This document requires the following approvals:

Name & Title	Date of Approval	Version
Force Policy Officer	12.05.2021	4.0
Deputy Chief Constable	N/A Minor amendments only	
JNCC (Not required for all policies)	N/A	

Distribution:

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		
Other: (state method here)		

Diversity Impact Assessment:

Has a DIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the DIA with the policy.	☐ Yes ☐ No Date:
---	---

Consultation:

List below who you have consulted with on this policy (incl. committees, groups, etc):

Name & Title	Date Consulted	Version
Neil COWLING (ISO), Jonathan JONES (ICTSO)	January to May 2021	4.0
Laura NORTH (DPO), Leonie CALLAND (Records Manager)	January to May 2021	4.0

Implications of the Policy:

Training Requirements

None

IT Infrastructure

None