CLEVELAND
POLICE

Information Security Policy

Policy Number	162
Policy Owner	Head of Standards and Ethics
Version	2.3
Last Review Date	January 2022
Next Review Date	October 2024
Date of approval	5/3/19
Protective Marking	Official

This document has been assessed for:	
Compliance with Legislation	☒
Equality Impact Assessment	Not required
Freedom of Information issues	☒
Human Rights compliance	☒
Health and Safety	☒
Risk Management	☒

1. Statement

This policy specifies the minimum measures required to protect the confidentiality, integrity and availability of police information assets, while enabling staff to perform their duties with an acceptable level of risk. This is necessary to protect individual staff, maintain public confidence and ensure that we fulfil our obligations to other stakeholders.

Cleveland Police has identified five strategic information security risks:

1. loss/disclosure of paper documents;
2. loss/disclosure of removable media;
3. inappropriate disclosure electronically (e.g., email, social media);
4. availability of critical computer systems; and
5. physical security of sites.

This policy applies to

- all officers and staff of Cleveland Police, including Special Constables and volunteers;
- all staff of the Police and Crime Commissioner's office;
- all staff of partner agencies with any access to Cleveland Police assets; and
- any other person given access to Cleveland Police assets.

In this policy, "staff" covers all those specified above.

2. Purpose

This policy is supplemented by Security Operating Procedures (SyOPs) and guidance documents. These SyOPs and guidance are updated more frequently than the main policy to reflect the changing facilities, resources and risks. The SyOPs and information security guidance can be found at the Information Security intranet.

The Information Security Manager and Data Protection Officer can be consulted for further advice regarding information security and data protection matters.

3. General duties applying to all staff

All staff have a responsibility to protect force information assets from all threats, whether internal or external, deliberate or accidental, thereby minimising the risk of disruption, compromise, harm or damage. All staff **must**:

- be aware of practices, risks and protective measures which concern them personally;
- ensure they have sufficient authority to access information and systems;
- comply with relevant laws, policies and standards; and
- inform supervisors of any relevant issues, circumstances or weaknesses in security arrangements.

Police information systems **must** be used for official police business **only**. All staff **must** comply with the security operating procedures applying to any particular activity, process or system, including the general SyOPs.

Personal devices (e.g., computers, laptops, mobile phones, USB storage) **must not** be connected to any police device or network. Personal devices **must not** be used for accessing, storing, transmitting or processing police information. Police information **must not** be emailed, transferred, photographed, or copied by any means to any non-Cleveland police system **except** as part of official police business.

Staff **must not** allow or permit any unauthorised person to use police devices or equipment.

Staff are personally responsible for securely handling any and all information they process in any way. Supervisors **must** ensure their staff are complying with this policy.

4. Information security training

All staff **must** complete all required training as specified in the general SyOPs.

5. Document and asset handling

5.1 Classification scheme

The Government Security Classifications (GSC) scheme applies. All staff **must** apply appropriate classification markings and ensure protection of information assets appropriate to the classification markings.

Additional requirements apply for those handling material classified at SECRET and above.

5.2 Clear desks, clear screens

Confidential or sensitive information **should** be kept out of sight when staff are away from their desk for a short time. When away for a longer period and at the end of each day/shift, this information **must** be stored securely in appropriate locked storage.

Computers, tablets and other devices **must** have a screen lock applied whenever unattended by the logged-in user.

5.3 Paper documents

Staff **should not** print documents unless a hard copy is necessary.

Staff **must** take only the smallest possible number of documents required out of police buildings.

Particular care should be taken when posting documents. Staff **must** check the appropriate address is being used and the envelope is endorsed according to the information enclosed.

Staff **should** adopt a “scan-and-shred” (or “scan-and-bin” via confidential waste bins) approach to paperwork; information from documents should be entered or scanned to a computer system and the original paperwork destroyed. This applies **except** where other policies or legal obligations require retention in original paper form (e.g., pocket notebooks).

5.4 Day books

Computer or electronic notebooks **should** be used instead of paper records whenever possible. Police-issue pocket notebooks or day books **must** be used instead of personal notebooks for police information.

5.5 Use of removable media

This section replaces the Removable Media Policy (policy number 257 version 1.3).

“Removable media” includes, for example:

- optical media (CDs, DVDs);
- external hard drives (usually connected via USB);
- USB memory sticks (a.k.a. pen drives or flash drives) and memory cards (e.g., SD/SDHC/SDXC/CF cards);
- devices with onboard memory, such as digital cameras and dictaphones; and
- backup media (e.g., digital tape).

Removable media **must not** be used unless no other reasonable method of data transfer can be found. Seek guidance from the Information Security team if in doubt.

Removable media **must** be scanned for malware as specified in the general SyOPs.

Removable media **must** be appropriately erased after each use.

5.6 Removable media encryption

Staff **must** ensure files written to removable media are encrypted. Where a system cannot produce encrypted media, the resulting removable media **must** be physically protected. **Exception:** files and data that are immediately intended for public distribution or where there would be no adverse impact should they be disclosed widely **may** be stored on removable media without encryption.

Encryption passwords **must** be strong passwords (see the passwords SyOPs).

Encryption passwords **must not** be sent with the associated encrypted removable media.

Staff **must not** rely on flash memory-based removable media for long-term storage of information.

5.7 Registration of removable media

Removable media of the types specified in the general SyOPs **must** be registered.

5.8 FAX machines

FAX machines **should not** be used unless there is no reasonable alternative. If used, ensure the correct phone number is entered and arrange for the proper recipient to be available to collect the FAX on its arrival.

6. Physical security

6.1 Site security

Staff **must** safeguard their warrant/ID cards and any other keys or access control tokens issued to them. Warrant/ID cards **should** be worn and clearly visible at all times while on Cleveland police premises.

Staff **must** consider the risk of “tailgating” through doors or vehicle gates.

Visitors **should** be escorted at all times **unless** they have a confirmed, current and sufficient level of vetting **and** have a suitable warrant/ID card or visitor badge which is worn and clearly visible.

Staff **must** take appropriate action if they suspect an unauthorised person is in a non-public area of a site or building, or if they identify an issue with the perimeter of a site or building.

6.2 Physical security of computers

Portable devices (e.g., laptops) **should** be locked away when not in use.

Staff **may** take portable devices home if relevant to their role. Business continuity plans might require some staff to take portable devices home.

Removable media **must** be stored securely in appropriate locked storage.

6.3 Transport of paper documents and removable media

Documents and other information assets **must** be transported with appropriate physical security measures.

7. Accounts, authentication and passwords

Staff **must not** share their accounts or passwords with any other person. Staff, including ICT and support staff, **must not** ask other staff to disclose their passwords.

Passwords **must** be sufficiently complex (see the passwords SyOPs).

It is generally accepted in the security community that it is better to use different, strong passwords for each account even if it means writing down those passwords. Staff **may** write down or store passwords electronically **if** they are sufficiently protected and not obviously associated with, or stored near the computer or device concerned. Stored passwords **must** be stored securely.

8. Internet access

Staff **must not** visit web sites concerned with pornography of any sort, promoting any kind of activity which is illegal or of doubtful legality, or promoting hate or disrespect for any individuals or groups while using a police device or network **except** when conducting lawful police business. Other policies and guidance (e.g., open source research) applies to such work.

Staff **must not** access social media services via police systems **except** in compliance with the Social Media & Electronic Communication Guidance.

Computer, network and Internet access is monitored.

8.1 Email

Emails concerning police business **must** be conducted using **only** official police email accounts. Personal email accounts **must not** be used for police business. Emails **must not** be automatically forwarded out of police email systems.

Police email accounts **must not** be used for personal matters (e.g., non-police mailing lists, personal shopping). **Exception:** this does not apply to matters directly relating to your employment such as emailing electronic payslips or certificates to a personal account.

Staff **must** exercise caution in handling email.

If sending sensitive email (e.g., a witness statement) to an external (non-Cleveland) address, staff **should** confirm the email address first (e.g., by asking the prospective recipient to email you first).

8.2 Video conferencing and instant messaging

Video conferencing services **may** be used. Such use **must** be in accordance with the teleconference SyOPs.

8.3 Personal use

Staff **may** have limited personal use of police computers for web browsing. Such use **must not** interfere with police business or cause any disruption to others.

9. Disposal

Information assets **must** be disposed of securely.

As soon as paper documents are no longer required, staff **must** dispose of them via cross-cut shredders or confidential waste bins at the earliest reasonable opportunity.

Staff **should** frequently check paperwork held in folders and other storage areas inside police buildings and destroy paperwork as soon as possible. The Records Management Retention Schedule applies and **should** be consulted.

Electronic storage devices (including hard drives and removable media) **must** be physically destroyed.

Redundant warrant/ID cards **must** be physically destroyed. This includes those where a replacement is issued and where staff have left the organisation.

10. Remote access

This section replaces the Remote Access Policy (policy number 236 version 1.3).

“Remote access” covers any access to a police system from outside a police building. This includes smartphones, tablets and laptops (collectively “remote access devices”).

All remote access devices **must** be encrypted.

Staff **must not** connect a police remote access device to any network **unless** it is a police network or a home network under the control of that person.

When working in public view, staff **must** ensure that police assets cannot be seen or accessed by others nearby.

Remote access **must** be in accordance with the remote working SyOPs and remote working overseas SyOPs.

11. Security incidents

A security incident is any actual or suspected failure in information security, including but not limited to:

- accidental or deliberate unauthorised destruction, modification or disclosure of information;
- unintended or deliberate unauthorised unavailability of the system;
- unauthorised access to systems;
- misuse, theft or loss of data or assets
- loss of removable devices;
- disclosure of or requests to disclose passwords; and
- any unauthorised entry to non-public areas of police premises,

and any attempt to cause such an incident.

Incidents **must** be reported to both a supervisor **and** via the process specified in the general SyOPs as soon as possible and within 24 hours of first becoming aware of the incident.

Near-misses **should** be reported by contacting a supervisor and the Information Security team.

Additionally, the misuse, loss, theft or compromise of the following **must** be reported as a security incident: pocket notebooks, day books, removable media, warrant/ID cards, Airwave radios, mobile phones, mobile working devices and computers.

12. Exceptions, violations and enforcement

Non-urgent exceptions to this policy should be sought from the Information Security Manager in advance. Decisions that could be seen as a violation of this policy or the association documentation **must** be recorded and reported to the Information Security Manager. Staff **should** apply the national decision making model when making such decisions.

Violations of this policy could result in disciplinary action or criminal prosecution.

The Senior Information Risk Owner (SIRO) and/or Information Security Manager **may** determine that particular actions or omissions are not a breach of this policy, taking into consideration relevant risks and requirements.

13. System Management

13.1 Procurement

New computer equipment and removable USB storage media **should** be procured via normal procurement channels in consultation with ICT.

13.2 New/modified information systems

New information systems **must** be procured via normal procurement channels and **must** include a Data Protection Impact Assessment and consultation with both the Information Security Manager and the Data Protection Officer **before** implementation.

Any change to an existing information system that might change a previous data protection or information security assessment **must** be notified to the Information Security Manager and the Data Protection Officer **before** that change.

13.3 Installation of software

Users **should not** install software unless they are in a system administration role and are complying with the prevailing policies, procedures and guidance.

13.4 Malware protection

All Cleveland police systems **must** have appropriate malware protection.

13.5 Change control

All aspects of Cleveland police's ICT infrastructure are subject to change control. This includes software, configuration (other than trivial desktop or application user configuration) and networks. Staff **must** conform to change control processes. Records **should** be retained for inspection by supervisors, the information security manager or auditors.

13.6 General requirements

Where technically feasible, computers and devices **must:**

- enforce appropriate password controls (concerning setting, expiry, reset and complexity);
- ensure sufficient protection of information both in-transit and at-rest;
- apply the principles of “least privilege” and “data protection by design and by default”; and
- be appropriately patched and monitored.

Additional requirements may apply outside the scope of this policy depending on the privacy and security assessments of a system/process.

13.7 Authority to operate

Information systems must receive authority to operate from the Data Protection Officer and Information Security Manager prior to operation or significant change.

14. Interpretation

“Must” conveys a requirement of this policy. “Must not” conveys a prohibition in this policy.

“Should” is a (strong) recommendation, and “should not” is a (strong) recommendation against something. Staff need to understand the implications before not conforming to “should” or “should not”.

“May” gives permission to do something but does not require or compel.

15. Appendix

Appendix	Description
1.	Legal and regulatory framework

16. Compliance and monitoring

The Head of Standards and Ethics is responsible for the accuracy and integrity of this document. This policy will be continuously monitored, and updated when appropriate, to ensure full compliance with legislation.

The Head of Standards and Ethics will review this process to ensure that all aspects are being adhered to in accordance with the framework of this policy.

17. Version control

This policy will be reviewed and updated at least every three years by the owner, and more frequently if necessary.

The Corporate Services Department will ensure this document is available on the Force intranet, including any interim updates.

The following identifies all version changes.

Version	Date	Reason for update	Author
0.1	31/1/10	Annual review together with a requirement to include Identity and Access Management (IAM)	[redacted]
0.2	Aug 2012	Review/revision of Policy	[redacted]
0.3	Sept 2012	Policy submitted to CBM following consultation	[redacted]
0.4	Oct 2012	Slight amendment to section 3.4 to correct Steria processes, resubmitted to CBM.	[redacted]
1.0	October 2012	Policy Approved at CBM	[redacted]
1.1	Nov 2012	Policy amended to reflect introduction of PCC, statement only	[redacted]
1.2	May 2017	Policy review and extension	[redacted]
1.3	Sept 2017	Change of owner department name	[redacted]
1.4	Dec 2018	Major rewrite to consolidate and update information security policies, implementation and guidance. Replaced/incorporated the Remote Access Policy (policy number 236 version 1.3) and the Removable Media Policy (policy number 257 version 1.3).	[redacted]
1.5	Jan 2019	Policy slightly amended to incorporate comments made during consultation.	[redacted]
2.0	Mar 2019	Policy approved at Chief Officer Group and published on the policy site	[redacted]
2.1	Jan 2020	Policy review – slight amends: • training requirements updated in s4 • info re: sheepdips updated in s5.5 • new s5.8 re: FAX machines • additional remark in s6.3 re: internal post • remark just above 8.3 re: cloud downloads • new procedure at end of s10 re: remote working SyOP • new impl note at end of s11 re: blocking missing items	[redacted]

		• new remark re: DPIA and security screening templates in 14.2	
2.2	Oct 2021	Remove implementation aspects, remarks and procedures to general SyOPs. Remove section re: ISB as governance is directed by the SIRO. Reorganise removable media sections. Add “authority to operate” requirement. Clarify use of email and personal use of web browsing. Emphasise day books over personal notebooks. Clarify incident definition. Minor textual changes for clarification. Link some SyOPs where directly relevant in text.	[redacted]
2.3	Jan 2022	Update hyperlinks following SharePoint site move.	[redacted]

Appendix 1

Legal and regulatory framework

Relevant legislation

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Crime and Disorder Act 1998
- Data Protection Act 2018 (GDPR)
- Freedom of Information Act 2000
- HMG Government Classification Scheme (currently version 1.1, May 2018)
- Health and Safety at Work Act 1998
- Human Rights Act 1998
- Investigatory Powers Act 2016
- Official Secrets Act 1989
- Police and Criminal Evidence Act 1984
- Regulation of Investigatory Powers Act 2000

Requirements and guidance

- GDS codes and guidance
- ISO27001 family of standards
- NCSC and CPNI guidance
- NPCC (formerly ACPO) guidelines
- NPIRMT codes and guidance