CLEVELAND POLICE

Information Security Policy

Policy Number	162
Policy Owner	Head of Standards and Ethics
Version	2.1
Last Review Date	January 2020
Next Review Date	January 2022
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	☒

Information Security Policy

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 and its associated implementation, "staff" covers all those specified above.

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

2. Purpose

This policy will be available with its associated implementation, procedures and remarks. The intention is that this associated information is updated more frequently than the main policy to reflect the changing facilities, resources and risks.

Remark - There is a varying level of detail in the implementation notes and procedures. Some topics require detailed, specific advice (for example, regarding acceptable encryption software) or relate to particular business areas. Others simply require a link to other existing documents.

Implementation, etc. - are distinguished from policy by a long bracket next to the text.

The Information Security Manager and Data Protection Manager 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 data 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 system.

Personal devices (e.g., laptops, mobile phones) **must not** be connected to any police device or network. Personal devices **must not** be used for the storage or processing of police information.

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 accompanying implementation note.

Implementation
The minimum for all staff is completion of the following e-learning packages available via NCALT:

- Managing Information (operational or non-operational as appropriate to role)
- Protecting Information level 1
- Government security classification

This training must be completed at least every two years.

Information Asset Owners must also complete

- Protecting Information level 2

5. Document and Asset Handling

5.1. Classification scheme

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

Implementation
The current Government Classification Scheme is described at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf.

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 screenlock 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.

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).

Remark
Scan-and-shred is strongly encouraged: most paperwork can be replaced by a computer record via data input or by scanning. Scan-and-shred also applies to criminal case paperwork with few exceptions. The most notable exception concerns pocket notebooks and the ELBOWS mnemonic.

5.4. Day books

Computer or electronic notebooks **should** be used instead of paper records whenever possible.

Implementation
The manila day books (first issued in 2018) have detachable pages to support "scan-and-shred" as described in the policy. Any page with sensitive information should be detached, scanned to a computer system, then securely destroyed. This reduces the risk of a large volume of paper-based information being disclosed if the book is lost.

The "blue" day books previously in use will be retained centrally: contact the Data Quality Coordinator for further guidance.

It is reasonable for staff to keep blue books if there is a business need (e.g., ongoing investigations). In this case, books must be clearly labelled —officer/staff, location, date started— and should be kept in police premises whenever possible, preferably in a locked cabinet when not in use. Each business area/team **should** keep a record of which staff have retained blue books.

Computer notebooks (e.g., OneNote or other editors), direct entry to computer records (e.g., Niche OELs) and electronic notebooks (as/when rolled out via agile working programmes) are alternatives to the use of day books (regardless of format).

5.5. 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).

Staff **must not** use any form of removable media unless no other reasonable method of data transfer can be found.

Staff **must** ensure all removable media is scanned for malware as specified in the accompanying procedure.

Procedure
Malware scanning for removable media

Removable media **should** be scanned using a "sheepdip computer" **before** connection to any other police system.

There are a very limited number of standalone "sheepdip" computers that can be used to scan removable media for malware prior to connection to another police computer. A list of sheepdip computers can be found via the Information Security intranet page.

Remark
If a sheepdip computer cannot be located to import or scan data from removable media, please inform the Information Security Manager. This enables recording of how often it is a problem and, if necessary, provide the evidence required to provide more sheepdip machines.

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.

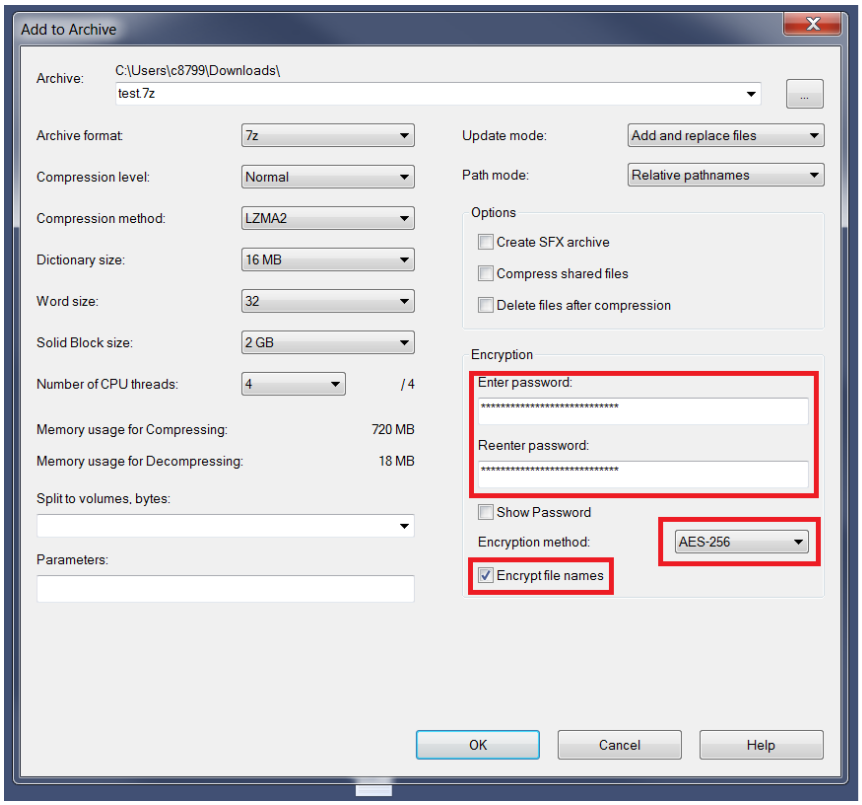
5.6. Removable media encryption

Procedure

Lumension is currently installed on police systems and can be used to write encrypted USBs, CDs and DVDs. Some instructions for using Lumension are available at http://intranet/CorporateInformationSites/encryption/SitePages/Home.aspx.

Lumension may not be suitable for larger media, particular USB hard drives. In this case, Bitlocker or Veracrypt are acceptable.

Encryption using the "7-Zip File Manager" is an acceptable form of encryption, provided the "Encryption method" is set to "AES-256" and "Encrypt file names" is ticked. The screenshot highlights those two requirements as well as the password box.



Always check that the file/device has been encrypted!

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

Implementation

Encryption passwords should be strong passwords. Ideally, use a password generation program.

Passwords for sharing encrypted media with CPS are available at: http://intranet/CorporateInformationSites/encryption/SitePages/Home.aspx.

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 associated implementation note **must** be registered.

Implementation
This requirement applies to:

- Dictaphones with onboard unencrypted storage — recorded by team supervisors.
- Unencrypted removable media for digital cameras used by SOCOs — recorded on "Lima".

The registers **should** contain enough detail to identify each item and its current location.

Implementation
Removable media authorisation

Any staff who require access to removable media for a business purpose will be granted that access. Further authorisation from the Information Security Manager used to be required, but is not required now. Complete the "Standard Request for Removable Media" form at:

http://intranet/TeamSites/steria/ICTServices/ICTSRs/Lists/RemovableMedia/Item/newifs.aspx.

Procedure
SARC ABE interviews

This section replaces the SARC Removable Media Guidance (version v1.1).

While it is technically infeasible to produce encrypted master copies, staff **must** ensure only one unencrypted disc (the master copy) is burnt from Sexual Assault Referral Centre (SARC) Achieving Best Evidence (ABE) interviews. Staff **must** check this master copy disc is viewable before it is taken from the SARC as the recording is held on the system for a short time only. SARC ABE interviews attract a classification of OFFICIAL-SENSITIVE.

Working copies **must** be encrypted. Working copies can be requested through the Property Store who will ensure they are encrypted using Lumension.

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 **should** 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.

Implementation
"Appropriate action" depends on the circumstances. A lone member of staff might reasonably choose to telephone the control room. An insecure door should be closed and if it cannot be properly secured, facilities should be called to provide a repair.

6.2. Physical security of computers

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

Remark
This recognises that furniture or facilities may not always allow this.

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

Implementation
The risks to portable devices are greater when they are transported. Staff should consider carefully where they store devices when away from police premises. In particular, they **must** be stored out of sight when transported in vehicles.

Removable media (described above) **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.

Implementation
Staff **must** consider the impact of loss/disclosure of paper documents or removable media when deciding on an appropriate means of transport. They **must** be stored out of sight when transported in vehicles.

For example, encrypted media **may** be sent via normal channels. Particularly sensitive media, even if encrypted, **should** be transported by hand or sent via special/recorded delivery. A locked case may be appropriate.

Unencrypted ABE interview discs **should** be transported by hand on a **direct** journey and not left unattended at any time.

Internal post should be properly labelled and packaged. Further guidance is available via the Information Security intranet page.

7. Accounts, Authentication and Passwords

Staff **must not** share accounts or passwords with any other person.

Passwords **must** be sufficiently complex. Staff **may** write down or store passwords electronically but those passwords **must** be stored securely.

Implementation
Guidelines for selecting a strong password:

- Make your password easy to remember but difficult for others to guess. Using the initial letters of a phrase is a common technique (e.g., "**m**ake **y**our **p**assword **e**asy **t**o **r**emember" becomes "mypetr").
- Passwords should have a minimum length of nine characters and should not be a dictionary word in any language.
- Passwords should contain a mixture of letters (upper- and lower-case), numbers and symbols.

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 passwords **if** they are sufficiently protected and not obviously associated with, or stored near the computer or device concerned.

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.

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

Implementation

Email (mis)addressing

A common security incident concerns misaddressing emails. Autocomplete is currently enabled on Outlook: staff **must** double-check that emails are being sent to the correct recipients before sending. Recall of emails is extremely unreliable.

Email and malware

Many viruses and malicious attacks are transmitted by email. Spam emails and phishing emails are common.

- Staff **must not** open unexpected attachments (even from known contacts, as the sender's address may be forged).
- Staff **must not** click on links in emails unless they are trustworthy.
- Staff **must not** (re)send chain mails as they are a channel for distributing malware.

Spam and phishing emails **should** be forwarded to the spam_email mailbox. If staff believe they have been compromised by such an email, they **must** treat it as a security incident.

Be aware that emails can be misconstrued and lead to misunderstanding and offence. Always re-read an email before sending it and ensure it reflects the message you are trying to communicate.

8.2. Video conferencing and instant messaging

Video conferencing services **may** be used. Such use **must** be in accordance with the associated implementation note. The "Installation of software" section of this policy is relevant if a service requires particular software.

Implementation

"WebEx" is provided for local use. There are many external video/web conferencing services. Regardless of the service in use, staff **should** exercise caution.

- It is difficult to verify the identity of other participants.
- Ensure the microphone cannot record any conversations that are not intended for the other parties.
- Ensure that any camera in use cannot view anything other parties are not permitted to see. Particular examples include whiteboards or documents with sensitive details.
- Ensure that any sharing of computer desktops does not reveal anything that other parties are not permitted to see. Even filenames can given away sensitive information.
- Staff **should not** allow remote control of their computers.

- As with other electronic communication methods, exercise caution in sending and receiving files via conferencing services and follow the requirements of the Government Security Classifications scheme.

An instant messaging service is provided for internal use **only**.

Remark
The current instant messaging service is Cisco's "Jabber". Staff should not attempt to use Jabber to initiate connections outside of the police network.

Remark
Downloading from cloud services

Staff sometimes need to download files from cloud services (e.g., when shared by partner organisations). If you find the links are blocked, please inform the Information Security Manager. This enables recording of how often it is a problem and, if necessary, provide additional means of accessing these services.

8.3. Personal use

Staff **may** have limited personal use of the Internet from police computers. 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.

Procedure
Optical media (CDs, DVDs) can be destroyed in some shredders. Check the shredder's instructions label first!

Other removable media (including USB sticks) and hard drives from decommissioned machines should be destroyed centrally. Contact SSC.

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.

Implementation

Authorisation

Any staff who require remote access for a business purpose (as verified by their line manager) will be granted that access. Further authorisation from the Information Security Manager is not required.

Additional authentication/confidentiality

Where a remote access device is connecting via a non-police network (e.g., a home wifi router), two-factor authentication is required. The precise details depend on the configuration on the device.

Devices intended for mobile working (such as smartphones) are pre-configured by ICT to a suitable level of network protection.

Public view

Extra precautions have to be taken when a computer which holds police assets is used in a public place such as a train. To avoid "shoulder-surfing" staff should ensure no one can see entry of usernames/passwords or the information displayed.

Procedure

Remote working security operating procedure

The remote working security operating procedure provides additional instructions for the handling of computers and smartphones.

11. Security Incidents

A security incident is any actual or suspected failure in information security, including:

- 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; and
- loss of removable devices,

and any attempt to cause such an incident.

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

Procedure
Security incidents **must** be reported via the online form at http://iis-police/Security/incidentintro.asp.

Near-misses **should** be reported via the process specified in the accompanying procedure.

Procedure
Near-misses **may** be reported via the same form, or by email to the Information Security Manager. Near-misses are useful information as they indicate potential threats that can be addressed before a security incident occurs.
Because of their oversight of ICT support tickets, ICT support staff **should** submit reports when a single event or a series of events suggests a possible risk to security.

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.

Remark
Prompt reporting of security incidents is vital because Cleveland police has a number of legal and regulatory obligations. For example,

- individuals may suffer harm if corrective action is not taken quickly;
- loss of personal data may require a notification to the ICO within 72 hours;
- further incidents may occur (perhaps unnoticed for some time).

Security incident and near-miss reports also inform the assessment and management of information security risks.

Implementation
Lost warrant/ID cards also need to be blocked. Lost computers, phones and radios are blocked by contacting the shared service centre or (out-of-hours) the control room, who will arrange for them to be blocked.

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 accompanying implementation **must** be documented 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. Information Security Board

The terms of reference of the Information Security Board (ISB) are:

- To identify the need for policies and advice on policy development in regard to complying with the [national] Community Safety Policy (CSP), other information security issues and in line with the strategic aims of the Force.
- To provide an arena where issues of concern can be raised and addressed corporately and at a strategic level.
- To receive from our strategic partner minutes from their Information Security Forum and direct action if required.
- To ensure the Force is kept up to date in regard to new legislation and case law.
- To disseminate areas of best practice.

14. System Management

14.1. Procurement

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

14.2. 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 Manager **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 Manager **before** that change.

Implementation
"Data protection by design" is a requirement for new information systems.

There is a general intention that a secure development lifecycle will be in place for all systems and software. It is accepted that some commercial off-the-shelf and open source software will not conform to this. Alternative mitigation or additional assessment will be required, depending on the scope of usage and relevant threats.

The data protection impact assessment template can be found via the Information Security intranet page along with a security screening questionnaire.

14.3. 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.

Remark
The general expectation is that ICT **should** install any software where a user has a well-founded business need and there is no adverse impact on systems, other users or the organisation overall.

14.4. Malware protection

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

Remark
There are some circumstances when the appropriate malware protection is "none", provided that the context and risk assessment supports this position.

14.5. 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.

14.6. 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 principle of "least privilege"; and
- be appropriately patched and monitored.

Remark
Password complexity and the associated controls depend on the system concerned and its threat environment.

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

15. 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.

16. Appendix

Appendix	Description
1.	Legal and regulatory framework

17. 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 Information Security Manager is responsible for the accuracy and integrity of **implementation** elements (including procedures and remarks) of this document. These will be continuously monitored, and updated when appropriate.

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.

18. Version control

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

The Performance, Quality and Review Team 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	[redacted]

		correct Steria processes, resubmitted to CBM.	
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 • new remark re: DPIA and security screening templates in 14.2	[redacted]

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