HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

POLICY

FORCE INFORMATION SECURITY POLICY

Governance:	**Senior Leadership Team**		
Document Type:	**Policy**		
Policy Owner:	**Chief Information Officer**		
Department:	**Finance and Resources**		
Policy Writer:	**Head of Information, Standards and Compliance**		
Policy Number:	**016**	**Version:**	**3.0**
Effective Date:	**01/11/2021**		
Recommended Review Date:	**01/11/2023**		

CHANGE HISTORY			
Version No	**Author**	**Changes**	**Ratification**
2.3	Head of IS&C	New document structure & review	Ratified at C.O.G. 17/7/09 subject to the inclusion of clarification in respect of point 9.6. Inserted 17/7/09 and agreed with Ch Supt Sandham (CIO).
2.3	Head of IS&C	Changes to point 11 to include gross misconduct references and insertion of point 23, which provides clarity.	Agreed at Change Committee 19/8/10.
2.4	Head of IS&C	Bi-Annual review & amended to take account of Force structure changes	Agreed at Change Committee 21/4/11.
2.5	Head of IS&C	Cosmetic changes made to reflect transition from Police Authority to Police & Crime Commissioner	Agreed by CIO
2.6	Head of IS&C	Inclusion of Information Asset Owners & associated responsibilities; reference to the Information Commissioner & reporting security incidents; reference to 2 NWP procedures.	Agreed by CIO 20/5/13
2.7	Head of IS&C	Annual review with minor cosmetic changes.	Agreed by CIO 30/07/2014
2.8	Head of IS&C	Reference to Management of Police Information (MoPI) amended to Authorised Professional Practice (APP)	Agreed by CIO 11/09/2014
2.9	Head of IS&C	Brief paragraph inserted to advise readers that this document is under review.	
3.0	Head of IS&C	Amendments after review & combining of the Force Information Standards Policy and Information Security Procedure	

CONTENTS

1. **WHY IS THIS POLICY REQUIRED?** 2
2. **WHO SHOULD USE THIS POLICY?** 2
3. **WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?** 2
4. **ROLES AND RESPONSIBILITIES** 9
5. **DECLARATION & LEGALITIES** 9
6. **APPENDIX A – 'Cloud' Information Security Risks** 11
7. **APPENDIX B – SECURE DISPOSAL OF POLICE INFORMATION** 13

1. WHY IS THIS POLICY REQUIRED?

The aim of this policy is to

- Facilitate the processing of personal data by North Wales Police (NWP), in compliance with the Data Protection Act 2018.
- Preserve the confidentiality, integrity, availability and non-repudiation of the information required by NWP, to enable their policing and related support function.
- Protect NWP information from malicious attacks and reduce the cyber and information risk to NWP information, the NWP network, electronic systems, servers, mobile devices and computers to an acceptable level.
- Ensure compliance with national Police information security and cyber risk policies.
- Ensure continued connection to national Police ICT systems & networks.
- Protect NWP information assets held electronically, digitally or manually, whether on premise or in a Cloud environment, from internal and external, technical and non-technical threats.
- Support the implementation of the North Wales Police Information Management Strategy.

2. WHO SHOULD USE THIS POLICY?

All Staff (uniform or non-uniform) and users with access to the NWP network and to NWP information and personal data, must read and comply with this policy.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

When this policy refers to information, this includes any type of work related information and personal data.

Only NWP owned and authorised computers, laptops and other mobile devices and media may be used to process NWP information; all must have adequate and documented asset control.

All NWP workstations, mobile and digital devices are provided for NWP work-related use only; no personal devices may be used for NWP work-related purposes.

It is not permitted to connect any personal devices such as smartphones or tablets to the NWP network for charging or for any other purpose.

Do not connect any non-NWP USB memory devices to the NWP network without first referring to IS&C for information security advice.

Staff are authorised to access and use information held by NWP, for their role-related work purposes only. You must not use, or permit the use of any NWP held information for private or non-work related use. Please be aware that the unlawful obtaining or disclosure of personal data or the selling of that data is an offence.

Any unlawful use of police data may render you liable to internal disciplinary action and legal proceedings, which could lead to a disciplinary finding of gross misconduct and loss of employment.

Where a personnel data breach is suspected, this will be assessed by the Professional Standards Department to determine a proportionate response which may result in gross misconduct or misconduct procedures. This assessment will be made on a case by case basis and will include consideration of all relevant factors.

If NWP information is compromised in any way, it could mean serious risks to:

- The lives of fellow Officers and Police Staff
- Informants
- The success of operations and investigations
- The public
- The reputation of the Force.

It is therefore imperative that we all keep our work-related information secure and reliable, whatever format it is held in (digitally, technically, manually; in paper format, in an email, photographic, DVD, USB device, SD card to name a few examples) and where it is accessed, for example from home or any other non NWP location. We also need to ensure it is available at the point of need for our work to be efficient and effective.

The security of NWP information and information assets will be achieved both proactively and reactively by implementing an appropriate combination of personnel, physical, procedural, technical and cyber controls; cyber and information risks will be assessed and mitigated to an acceptable and manageable level taking account of the business need.

NWP will use auditing, monitoring and the gathering of intelligence to assist with the identification of information security and data protection threats and vulnerabilities to keep NWP information secure and to detect unauthorised access. This is undertaken in accordance with legislation and in a controlled manner; there should be no expectation of privacy

If you are unsure about any aspect of information security, please contact the Information Standards and Compliance Team; this could be:

- in your day to day function
- a new project or initiative
- a new information sharing request or disclosure
- purchase or use of a new piece of ICT equipment or USB device
- responding to a request for information
- a new contract that involves using information or to support an ICT system
- considering using 'the cloud' to store or process police and / or personal information
- an information security incident or personal data breach – an incident waiting to happen
- a suspected information security vulnerability
- any information security aspect you would like to discuss, or you just want advice on

The movement of bulk data from one system to another or to another device or to another agency must be authorised by the Chief Information Officer.

Further guidance can be found in the tables and appendices in this document.

Access to NWP ICT, information and premises	Access to information systems and buildings will be limited according to the needs and role responsibilities of each individual. Visitors should sign in, be provided with a visitor pass card and be escorted. Procedures

	must be in place to ensure visitors leave a building and hand in their ID card. No photographs should be taken by visitors unless it is in line with their specific work e.g. architect; however, this should be agreed and authorised prior to any visit. In these cases, extreme care must be taken to ensure no personal or sensitive data is photographed. Access to information systems must be by way of individual user ID and password. Computer systems should ensure inclusion of sufficient built-in authentication; terminal logging and audit trails to determine all use of that system. **All NWP employees will be issued with a single user log on (SULO) and must successfully complete ICT system training, NWP vetting requirements and data protection awareness training prior to further access being granted to additional NWP ICT system(s) or information; there must be a business need.**
Access - 3rd Party Technical	Technical access to NWP network and systems must be for an agreed, specified business purpose. Adequate technical and procedural security must be ensured, to lockdown and control such access. **Access must be monitored and audited. Security controls must be agreed, implemented, and defined in any contract with the third party; data processing agreements must be signed.**
Business Continuity and Disaster Recovery	Disaster Recovery and business continuity plans must be documented, implemented, and regularly tested to **ensure effective recovery from a disaster or system failure and to ensure business continuity. These procedures must be practiced and reviewed regularly.** Routines should be established and documented for taking back-up copies of data and software, rehearsing its timely restoration, logging events and faults and monitoring the equipment environment. Any faults should be reported, and corrective action taken. Logs should be maintained to ensure that security procedures have been followed and all activities monitored e.g. system start and finish time, system error and type of corrective action taken.
Cloud Security Principles	More and more information is being placed on cloud solutions; for example Microsoft 365, Amazon Web Services (AWS), or via other companies providing data centre services. These bring a set of extra potential risks which must be considered to keep NWP data safe. A brief synopsis of these risks can be found at Appendix 1, but IS&C must be consulted before a decision is made to use 'cloud' services to ensure potential risks are identified and mitigations implemented. This is particularly important where there are any implications or connections to national police systems (e.g. PND, ANPR, PNC, VISOR etc.).

File Management	In order to assist with the availability of NWP information and for record management purposes, please ensure effective maintenance of information saved in Group and personal (H) drive folders. Public (P) drive, SharePoint Teams and other O365 tools are subject to its own procedures – please refer to the Record Review Dept Manager for further information about the management of drives or to ICT if you have any queries regarding backup of information saved on the drive.
Forensic Readiness	A Forensic Readiness procedure must be documented and agreed. This maximises the ability to preserve and analyse data generated by an ICT system that may be required for legal and management purposes. Computer/communication clocks must be synchronised. The NWP Forensic Readiness Policy can be access here.
Governance	NWP will have the following information security and data protection governance structure in place • The Chief Constable is the Data Controller. • The Director of Finance and Resource is the Senior Information Risk Officer (SIRO). • A Data Protection Officer will be appointed in line with legislative requirements. • An Information Security Board (ISB), chaired by the Chief Information Officer (CIO) will oversee information security and provide clear direction and visible management support for information security initiatives. • Each NWP ICT system will have a nominated Information Asset Owner (IAO). The IAO is responsible for ensuring 'their' asset's comply with this policy and ensuring adequate governance, risk management, change control, access controls and documentation is in place, taking account of the value of the information processed on their asset; reporting to the SIRO as directed and required and keeping IS&C aware of information security related changes, incidents and vulnerabilities. • Heads of business areas will be responsible for complying with and implementing this policy and its supporting policies, within their own areas, in respect of the information and the ICT systems business area uses. This includes ensuring that their practices and procedures comply with relevant ICT SyOPs (Security Operating Procedures) and any relevant information security risk-based decisions made by the CIO, the SIRO and the relevant Information Asset Owner (IAO). • Although some devolvement of responsibilities has taken place within NWP, the importance of Data Protection and Information Security standards remaining consistent is recognised and required.

Information Security Incidents	Information security incidents, personal data breaches and relevant vulnerabilities will be recorded via the Information Security Incident Procedure (SIP). NWP will consider each information security incident which involves personal data to see if it meets the Information Commissioner's (ICO) requirements for advising the ICO of this incident.
Legislation and Standards	NWP has adopted and will comply with: • The Data Protection Act 2018 • The Freedom of Information Act 2000 • The national NPCC Information Systems Community Security Policy (NPCC CSP) – this document can be accessed by contacting information.assurance@homeoffice.pnn.police.uk • The Government Security Classification Scheme • ITIL (IT Infrastructure Library Best Practice) North Wales Police will have regard to: • the guidance within Authorised Professional Practice (formerly Management of Police Information). North Wales Police will use: • the following standards as a benchmark and will comply with the requirements of any relevant codes of connection (e.g. PSNP, PNC, Airwave, PND, ANPR and VISOR) or policies to which NWP are signatories: (a) Security policy framework 2018 (b) ISO27001 Information Security Management (c) Industry Security Notices (ISN) (d) NCSC Risk management guidance (e) NPCC Vetting Code of Practice 2017
Mobile Computing	To ensure the security of data when using mobile computing, the protection required must be commensurate with the risks. The risks of working in an unprotected environment should be considered and appropriate physical protection, access controls, cryptographic techniques, back-ups, virus protection and documented security operating procedures must be in place to ensure that NWP information is not compromised. Mobile computing includes using laptops; Mobile phones, Tablets, USB Storage pens, Digital Voice Recorders (DVRs) and Body Worn Cameras (BWCs).

	All procurement of mobile devices must be centrally controlled and authorised by ICT. When procuring mobile technologies, where possible they should only include the technology expressly needed by NWP.
Outsourcing – Data Processor	Risk assessments must be undertaken and documented before the responsibility for information processing NWP information is outsourced to another organisation. Prior to any work being undertaken, a contract should be signed, containing details of the required adequate security controls, to ensure management of any information risks; where processing of personal data is to be undertaken on behalf of NWP this must also include a data processor agreement.
Personnel Security	Security responsibilities should be addressed at the recruitment stage, included in contracts and monitored during an individual's employment. The level of vetting or clearance of all personnel requiring frequent and long-term uncontrolled access to Protectively Marked assets should be proportional to the value of the asset being protected; the Government Security Classification (GSC) gives guidance about vetting levels. Please also refer to the Vetting Module on APP.
Physical Security	Physical entry controls and procedures to Police buildings, sites and locations should be adequate to ensure the security of the information/asset stored within (refer to GSC guidance) A defence in depth approach must be adopted, which will assist departments to ensure physical security is adequate Responsibilities and Physical Security: **Facilities (Finance and Resources)** are responsible for ensuring adequate physical security controls are considered and implemented for new and existing police buildings. They are also responsible for requesting advice in respect of any non-police buildings to be used which Facilities become aware of. **ICT (Finance and Resources)** are responsible for ensuring adequate security for NWP server rooms & IT equipment rooms, as detailed in the ICT Data Centre Access SOP. IAO & Business Area Leads are responsible for ensuring adequate security for information owned/ processed by them and that adequate physical security is maintained for the buildings/rooms which fall under their area of business.
Procurement, Purchase, Repairs and Disposal of hardware and software	**Purchase and Procurement** Purchase and use of hardware, software and mobile data devices must be agreed by ICT to ensure compatibility, support provision, capacity requirements and business needs are met. N.B. This is essential even if the IT system is not included within the ICT managed service. Procurement of data bearing peripherals such as USB memory devices and SD cards must be agreed by IS&C to ensure that appropriate asset control, Ivanti (previously known as Lumension) authorisation,

	encryption, processes and other information security and data protection issues are assessed and addressed. All information assets procured must be asset controlled and have a defined asset owner from the point of initial receipt in NWP onwards; regular asset control checks should take place. All data bearing devices must be disposed of securely via the NWP processes in place. Where necessary, additional consultation should be undertaken with ICT, to determine the best method for this to occur. For secure disposal please see Appendix B or contact IS&C for advice. Any new ICT system or other asset must have an IAO assigned prior to go 'live'. **Repairs** Repairs and maintenance of an information asset should be undertaken on NWP premises by suitably cleared personnel. If this is not an option, secure and permanent erasure of information held on an IT asset should be considered prior to it leaving NWP. If this is not possible, for any reason, contact IS&C for advice.
Agile Working	Please refer to Agile and Home Working Practice Guide for guidance. If you are authorised to undertake NWP work outside the UK, please remember you require specific permission from your business area head to take laptops, mobile/smart phones out of the UK; a detailed risk assessment must be documented prior to authorisation; please contact IS&C for advice regarding threats and security measures. If you are required to undertake NWP in shared premises, an adequate security assessment must be undertaken and documented. Remote ICT equipment, even when off-line, must be regarded as an extension of the workplace system. It requires the same effective levels of physical, technical and procedural security.
Secure Disposal	All fixed and mobile devices and media which are ready for disposal must be disposed of or sanitised securely in accordance with their respective GSC guidance and their terms of use and in accordance with HMG IA Standard No 5. Please see Appendix B for further information. This includes standalone computers (i.e. not connected to NWP (network) maintained by ICT or independently by departments (see below for further compliance requirements in respect of standalone computers). The contracting of any disposal companies and the procedures used for the secure disposal of all data assets must be centrally controlled. Reference must be made to ICT and IS&C in the first instance to agree any new or revised disposal contracts and procedures. Such companies must have proven security credentials and must be able to provide the standards required in HMG IA Standard No. 5 – Secure Sanitisation of

	Protectively Marked or Sensitive Information. Documented procedures must be in place and adhered to. Please be aware that digital photocopiers and Multi-Functional Devices (MFDs) incorporate embedded hard disks for the temporary storage of information and therefore pose a security risk.
Stand Alone Computers	All stand-alone computers (i.e. not connected to the NWP network but used for NWP related work) must be included on the NWP asset register. Where there may be ICT agreement for these to be locally managed, that management must include adequate information security controls. For the avoidance of doubt, standalone assets include: • Those provided by partnership funding, or similar. • Those introduced for use by NWP from seized property perhaps for CCTV viewing. • Obtaining a standalone outside the NWP procurement procedure. • Those provided via the NWP procurement procedure. All standalone computers should have whole disk encryption (Becrypt, Ivanti or Bitlocker) installed unless otherwise agreed with IS&C and ICT.
Training	All staff and users who have access to NWP information and/or NWP ICT systems and devices will be required to complete regular awareness training in the general principles of data protection and information security.
Web Site (NWP)	Adequate security and procedures must be in place to protect the integrity of electronically published information, to ensure compliance with the Data Protection Act 2018 and to prevent unauthorised modification which could impact on the integrity of the NWP information or harm the reputation of the Force.

4. ROLES AND RESPONSIBILITIES

4.1	Controller	The Chief Constable is the controller of all personal data held by NWP and determines the purpose of processing this data.
4.2	Senior Information Risk Owner (SIRO)	The SIRO has overall responsibility for managing risks to personal data held by NWP.
4.3	Information Asset Owner (IAO)	IAOs must ensure that their information asset is held securely, has appropriate governance documentation in place, and that the information is used to its full potential.

5. DECLARATION & LEGALITIES

5.1 In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall, the intention of this policy is to make North Wales the safest place in the UK.

5.2 In the writing of this policy cognisance has been taken of the college of policing code of ethics (2014).

5.3 North Wales Police policies will be written in accordance with the approved corporate format and published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.

5.4 The following main legal requirements have been identified within this policy:

- Equality Act 2010
- Human Rights Act 1998
- The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
- Data Protection Act 2018
- Freedom of Information Act 2000
- Health and Safety Act 1974

5.5 This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).

5.6 New legislative requirements or changes in Force structure may necessitate a review of this policy document.

6. APPENDIX A – 'Cloud' Information Security Risks

- Data in transit must be adequately protected against tampering and eavesdropping via a combination of network protection and encryption. If this is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.

- Asset protection and resilience. Data, and the assets storing or processing of it, should be protected against physical tampering, loss, damage, or seizure. If this is not implemented, data could be compromised which may result in legal and regulatory sanction, or reputational damage.

- Separation should exist between different consumers (tenants) of the cloud service to prevent one malicious or compromised consumer from affecting the service or data of another. If this is not implemented, cloud service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.

- The cloud service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it. If this is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.

- The cloud service provider should have processes and procedures in place to ensure the operational security of the service. If this is not implemented, the service can't be operated and managed securely to impede, detect, or prevent attacks against it.

- Cloud service provider staff should be subject to personnel security screening and security education for their role. If this is not implemented, the likelihood of accidental or malicious compromise of consumer (tenant) data by service provider personnel is increased.

- Services should be designed and developed to identify and mitigate threats to their security. If this is not implemented, services may be vulnerable to security issues which could compromise consumer (tenant) data, cause loss of service or enable other malicious activity.

- The cloud service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement. If this is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

- Consumers (tenants) should be provided with the tools required to help them securely manage their service. If this is not implemented, unauthorised people may be able to access and alter consumers' (tenants) resources, applications and data.

- Access to all cloud service interfaces (for consumers (tenants) and cloud service providers) should be constrained to identified, authenticated and authorised individuals. If this is not implemented, unauthorised changes to a consumer's (tenant's) service, theft or modification of data or denial of service may occur.

- All external or less trusted interfaces of the cloud service should be identified and have appropriate protections to defend against attacks through them. If this is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.

- The methods used by the cloud service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. If this is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.

- Consumers (tenants) should be provided with the audit records they need to monitor access to their service and the data held within it. If this is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.

- Consumers (tenants) have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected. If this is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.

- Cloud services operate internationally with the risk that police data could be stored/processed overseas. Failure to ensure it remains domiciled in the UK or EU (pending Brexit conclusions) could render the consumer (tenant) in breach of the Data Protection Act 2018, with associated sanctions and reputational damage.

- Multi-tenant or shared service clouds are attractive targets for malicious threat actors, whether they are organised crime groups, nation states or lone individuals. The possibility of disrupting police activity is an additional attraction for malicious intent.

7. APPENDIX B – SECURE DISPOSAL OF POLICE INFORMATION

7.1 Secure Disposal of Police Information

T**he** "deletion" of computer files and data, even after they have been removed from the systems "recycle bin" or equivalent, does no more than make the relevant storage area available for overwriting. Until the storage area is in fact overwritten, the "deleted" information can usually be recovered, with minimal expertise using the Commercial off the Shelf (COTS) utility software. For this reason the storage device must be securely erased in accordance with National Cyber Security Centre (NCSC) guidance Secure sanitisation of storage media - NCSC.GOV.UK. In addition to this NWP have the following procedures in place

All waste must be disposed of in accordance with this policy; subject to the Government Security Classification (GSC) scheme marking given to the information asset.

This appendix relates to the storage, transmission and destruction of the waste types stated in Table 1, which have a GSC of Official or Official Sensitive.

Advice must be sought from either the Force Special Branch, Force Intelligence Department, or IS&C in respect of assets marked as either SECRET or TOP SECRET.

Table 1: Waste Types:

Waste Type	**Waste Management Process**	
	Guidance	**Destruction Process**
Paper documents	Refer to Section 7.**2**	Secure destruction via Contractor
Magnetic Media (audio & video tapes; CDs, disks)	Refer to Section 7.**3**	Secure destruction via Contractor
Desktop IT equipment, servers, external HDDs etc	Refer to Section 7.**4**	Via Managed Desktop Service
Mobile phones	Refer to Section 7.5	Via Business Managers (process under review)
Airwave terminals	Refer to Section 7.6	Via Airwave Manager
USB sticks and similar small items such as SD cards etc.	Refer to Section 7.7	In house destruction
Photocopiers/ Multi-Function Devices (MFDs)	Refer to Section 7.8	Procurement
Digital Voice Recorders (DVRs)	Refer to Section 7.9	In house destruction
Body Warn Cameras (BWCs)	Refer to Section 7.9	Returned to supplier.

7.2 Paper Documents

All Force information as a minimum is classified as OFFICIAL (including handwritten notes), and will be disposed of in accordance with the secure disposal process operated and coordinated by Facilities Management Dept (see 7.3 Waste management procedure for the disposal of Documentation and Magnetic Media).

Briefly, this comprises the following: -

- All Force information upon disposal should be placed directly into a secure waste paper cabinet which is lockable and contains a slot in the top which allows enough room for paper to be fed through, but does not allow for access to the contents by hand. These cabinets should be available in every office area within NWP premises.

- Waste paper documentation with a government security classification of Official Sensitive may be torn by hand into small pieces and placed directly into a SECURE WASTE PAPER CABINET. More substantial quantities should be shredded using a CPNI approved cross cut shredder, which can be found at various locations within the Force. If a department is seeking to purchase a suitable shredder, please contact IS&C for advice.

- Departments, via their business managers, will have procedures in place to remove bags containing waste paper from the secure waste paper cabinets and place them in secure storage on NWP premises to await secure shredding by the appointed contractor.

- Each shred undertaken by the Contractor will be supervised and witnessed by a member of NWP personnel and the process recorded confirming that the waste has been securely destroyed on site; the date this occurred; the duration of the shred (time in and out); the number of bags shredded and the type of waste.

- Records of all shredding and subsequent disposal will be maintained by Facilities Management Department.

- Where members of NWP staff work on non-police premises such as partnerships offices or home locations, all GSC marked paper waste must be returned to the nearest NWP premises for secure destruction.

7.3 Magnetic Media

- The waste management process for MAGNETIC MEDIA (audio tapes, video tapes, CDs, & DVDs &) follows a similar process to that for waste paper, except that the initial collection of the magnetic media is via local arrangements within departments (see7.2 Waste management procedure for the disposal of Documentation and Magnetic Media). For further advice in this regard, please contact your business manager.

- Where members of NWP staff work on non-police premises such as partnerships offices or home locations, all magnetic media with a GSC marking must be securely returned to the nearest NWP premises for secure destruction.

7.4 Desktop IT Equipment, External HDDs, Servers etc.

- All destruction of IT equipment holding a GSC marking will be carried out in accordance with the NWP Computer Decommissioning Procedures under the NWP-CGI Desktop Computer Managed Service Contract. This will include all desktop IT equipment, laptops, servers, multi-function devices (with combined print copy, scan & fax capability) and independent external hard drives including any IT equipment

purchased by Departments directly and which is not supported under the Managed Service contract.

- All redundant hard disk drives (HDDs) not physically destroyed are secure wiped. Assets for disposal are then either re-cycled in accordance with the WEEE directive by an ISO accredited contractor or re-marketted. Additional provisions exist, where there is a specific requirement, for the destruction of equipment to be witnessed.

- This process complies with NCSC guidance and will provide secure destruction of information in electronic form up to and including SECRET.

- This process is owned and managed by ICT who will monitor and audit as necessary.

- No NWP IT information assets will be destroyed via any other process.

7.5 Mobile Phones

- The destruction or disposal of Force-owned mobile phones is organised by local business managers within Departments (process currently under review).

- Any information stored on a mobile phone or its SIM card (such as telephone numbers, calendar appointments etc) must be securely deleted before the phone is sent for disposal and this must be checked by the Department before disposal is authorised. This also includes SD cards which should be removed and disposed of as per Section 7.7 below as they can't be securely wiped.

- Departments will ensure that comprehensive records are maintained in respect of the issuing and management of mobile phones including records of disposal to enable independent auditing to be undertaken as deemed necessary.

7.6 Airwave Terminals

- The destruction or disposal of Airwave terminals is managed and controlled by the Control Room Systems Manager and CGI. Overt terminals are returned to Sepura while Covert terminal destruction is managed only by the Control Room Systems Manager, and carried out in accordance with national guidance.

- All obsolete or damaged terminals will be returned to Control Room Systems manager who will arrange for secure destruction or disposal where required.

- The Control Room Systems manager in ICT will ensure that comprehensive records are maintained in respect of the issuing and management of Airwave terminal equipment including records of disposal to enable independent auditing to be undertaken as deemed necessary.

7.7 Removable storage devices (such as USB sticks, SD cards, Flash memory cards and readers (SD, CF, MS, XD), Digital cameras with on board memory, or any other devices which may contain such removable storage media)

- Removable storage devices cannot go via the onsite secure destruction process used for waste paper and magnetic media due to their size and there is a probability of passing through the mobile shred unit's blades without being shredded.

- Departments will ensure that local procedures are implemented to ensure that removable storage devices for destruction are forwarded with relevant GSC marking (with details of the sender, location and information held on the device) to CGI (internal mail to be arranged via the SSF) who will arrange for them to be securely wiped of all information. They are then forwarded to the Archive to be securely destroyed.

- Departments will ensure that comprehensive records are maintained in respect of the issuing and management of removable storage devices including records of disposal to enable independent auditing to be undertaken as deemed necessary.

7.8 Photocopiers/MFDs

- Digital Photocopiers and MFDs incorporate embedded hard disks for the temporary storage of information and consequently the Force Procurement Department will ensure that contracts for use and repair take cognizance of the advice and guidance provided by NCSC.

- The Force Procurement Department will co-ordinate the disposal of photocopiers and ICT will manage the disposal MFDs with each department being responsible for ensuring that they are disposed of in accordance NCSC guidance.

7.9 Digital Voice Recorders and Body Worn Cameras

- All DVRs and BWCs which are damaged beyond further use and/or are outdated must be disposed of securely as they may hold GSC marked information.

- Departments will ensure that local procedures are implemented to ensure that the devices above due for destruction, are forwarded (with details of the sender, location and information held on the device) to CGI for DVRs or body worn video supervisor for BWCs (internal mail to be arranged via the SSF), who will arrange for them to be securely wiped of all information. CGI will then forward the wiped DVRs to the Archive to be securely destroyed and BWCs will be returned to supplier.

Departments will ensure that comprehensive records are maintained in respect of the issuing and management of these devices including records of disposal to enable independent auditing to be undertaken as deemed necessary.