WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Secure Sanitisation and Disposal**
POLICY REFERENCE NO:	**Inf/10**

Executive Summary.

In accordance with the HMG SPF Mandatory Requirement No 8 (MR8), West Midlands Police will ensure that Risk Assessments are carried out to identify, quantify and prioritise risks to all protectively marked information, information assets and personal data. Appropriate controls and proportionate measures will be selected and implemented to mitigate the risks identified.

***Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.*

Intended Policy Audience.

This policy applies to every police officer, member of police staff, police community support officer, special constable, volunteer, contractor, and approved persons working for or on behalf of West Midlands Police.

Current Version And Effective Date.	**Version 0.2**	**11/09/2014**
Business Area Owner	**Intelligence**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Paul Richards – Information Security Officer**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**17/10/2014**	
Review Date	**17/10/2016**	
Protective Marking	**Not Protectively Marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- *HMG Security Policy Framework (SPF);*
- *CESG IA Standards (IAS) and Good Practice Guides (GPG's);*
- *BS EN ISO27001 – Information Technology*
- *WMP Information Security Policy*
- *WMP Local Threat Assessment*
- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Diversity Vision Statement and Values

“Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values”

“All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay.”

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1. ABBREVIATIONS.

ACPO Association of Chief Police Officers
A/V Anti-Virus
ADS Accreditation Document Set (i.e. RMADS Risk Management Accreditation Document Set)
AO Accounting Officer (Chief Constable)
BC Basic Check
BCM Business Continuity Management
BCP Business Continuity Plan
BIA Business Impact Analysis
BS25999 Business Continuity Management - (BS 25999-1:2006) now ISO/IEC 22301:2012
CESG Communications-Electronics Security Group
CTC Counter Terrorism Check
CPU Central Processing Unit
DPA Data Protection Act 1998
DTI Department of Trade and Industry
HMG Her Majesty's Government
IAO Information Asset Owner
ICM Information Compliance Manager
InfoSec Information Security
ISF Information Security Forum
ISM Information Security Manager
ISO Information Security Officer (For the WMP Force)
ISO 22301 International Standards for Business Continuity Management - Requirements (ISO22301:2012)
ISO 27001 International Standard for Information Security Management System - Requirements (ISO27002:2005 contains the Implementation Guidance and Code of Practice)
IS Information Systems
ISP Information Security Policy
ISTU Information Systems Training Unit
ITIL Information Technology Infrastructure Library
LAN Local Area Network
NISCC National Infrastructure Security Co-ordination Centre
NPIRMT National Police Information Risk Management Team
PM Protectively Marked
RMADS Risk Management Accreditation Document Set
SC Security Check
SIRO Senior Information Risk Owner
SoA Statement of Applicability
SIIMN Strategic Information and Intelligence Management Board
SPF HMG Security Policy Framework
SyOPs Security Operating Procedures
SysOPs System Security Operating Procedures
System Information System
UNIRAS Unified Incident Reporting and Alerting Scheme.
UPS Uninterruptible Power
WMP West Midlands Police

2. TERMS AND DEFINITIONS.

Asset - An asset is something tangible or non-tangible which is of value to the organisation and needs to be protected, can be generally sub-divided into 'Primary Assets' and 'Supporting Assets'. **Primary Assets** are 'Processes' and 'Information Assets' used by, stored or communicated by the organisation. **Supporting Assets** are all other Hardware, Software, Networks, Utilities, Physical Premises, People and Organisational Structures that are present to make the use of the 'Primary Assets' possible;

Availability - Ensuring that authorised users have access to information and associated assets when required;

Confidentiality - Ensuring that information is accessible only to those authorised to have access;

Identity and Access Management - In information systems, identity management is the management of the identity life cycle of entities (subjects or objects);

Information Asset - An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation;

Information Security Policy - The set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed;

Integrity - Safeguarding the accuracy and completeness of information and processing methods;

Risk - The likelihood of a threat occurring and being successful in exploiting vulnerability, and causing a breach of security;

Security - A combination of confidentiality, integrity and availability considerations;

Evaluation - The assessment of an IS system or product against defined criteria;

Threat - The likelihood that an attacker will attempt, and has the capability, to exploit a vulnerability to breach security; and

Vulnerability - A feature of a system, which, if exploited by an attacker, would enable the attacker to breach security.

3. INTRODUCTION.

3.1. West Midlands Police must ensure that data and equipment that's holds data is correctly managed or sanitised before repurposing that data or equipment. An effective policy and framework of controls, covering classification, sanitisation and recording is required to protect critical information assets against known threats and reduce the overall risk to organisational operations.

3.2. This policy covers all components that hold or manage data including magnetic media, tape, Hard Disk, Compact disk/DVD and paper. If there is a technology not listed but guidance required this should be raised and escalated to the policy authors.

4. SECURE SANITISATION POLICY.

4.1. Formal documented standards and procedures, consistent with HMG IS5 'Secure Sanitisation' should be in place and cover the following:

- Asset management defining the type of storage device (including on-board solid state capability)
- Processes for the secure deletion of data to include Overwriting Degaussing and Physical Destruction
- Processes for the destruction of physical hardware or media (including management and storage of destruction certificates for audit purposes)
- recording and maintaining a register of critical and non-critical data types
- maintaining the accuracy of details in all supporting documentation
- the ability to perform regular checks to identify, investigate and resolve any discrepancies with physical assets and data classifications

Note: Only approved solutions may be used for secure sanitation of data as defined by CESG http://www.cesg.gov.uk

When is secure sanitisation required?

4.2. If reused or repurposed media does not meet all the following conditions then secure sanitisation of that media is required.

- The media is to be reused at the same classification, and
- Within the same secure environment (e.g. same team/solution), and
- Where no 'need to know' controls were previously in force.

Note; if sanitisation is not required devices must be subject to the erase function native to that operating system. Failure to complete should be recorded and risk managed.

IL3 or below

4.3. In the event of equipment being repurposed or 'end of life' which holds data that is marked as IL3 or below, the media must be either Overwritten or Degaussed or Physically Destroyed. If these activities are to be completed by a 3rd party then WMP staff must be present at all times (including transport, delivery and destruction) to oversee the process and obtain a destruction certificate once completed. Only approved solutions may be used for secure sanitation of data as defined by CESG http://www.cesg.gov.uk

IL4 or Above

4.4. In the event of equipment being repurposed or end of life that holds data that is marked as IL4 or above, the media must be either Degaussed or Physically Destroyed. If these activities are to be completed by a 3rd part then WMP staff must be present at all times (including transport, delivery and destruction) to oversee the process and obtain a destruction certificate once completed. Only approved solutions may be used for secure sanitation of data as defined by CESG http://www.cesg.gov.uk

Unknown

4.5. In the instance of media where the classification is unknown it should be treated as IL4 or above.

Paper

4.6. All paper must be incinerated or shredded. Paper destruction must either be through incineration or shredding in accordance with CPNI standards. If shredding is chosen then partials must not be larger than 2 x 15 mm.

CD/DVD

4.7. Destruction of all DVD or CD must be subject to a DVD splitter/Shredder before grinding or incineration.

Unacceptable Techniques for secure sanitisation

4.8. At no point is the use of encryption or Advanced Technology Attachment Secure Erase a suitable or approved method for secure sanitisation.

Non-Conformance and Exceptions

4.9. Non-conformance to this policy must be reported to the Force Information Security Officer. The Information Security Team must approve, track and report all exceptions to this policy in accordance with a formal documented process. The process should include a method for escalating significant exceptions that may breach a documented level of business risk tolerance, to the Security & Information Management Board in accordance with established governance procedures for review and mitigation or formal risk acceptance.

5. UNDERPINNING POLICIES AND PROCEDURES.

5.1. To support the overarching IA Risk Management policy the following policies will be maintained by the force –

1. Force Information Security Policy;
2. Information Management Policy;
3. Information Security Incident Management Policy;
4. Asset Management Policy;
5. Classification Policy;

6. EQUALITY IMPACT ASSESSMENT (EQIA).

6.1. The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how WMP has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

7. HUMAN RIGHTS.

7.1. This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

8. FREEDOM OF INFORMATION (FOI).

8.1. Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.2 of this policy has been GPMS marked as Not Protectively Marked

8.2. Public disclosure does not automatically apply to supporting Force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number

9. TRAINING.

9.1. This policy reflects best practice within ICT and IM and does not require a training element.

10. PROMOTION / DISTRIBUTION & MARKETING.

10.1. The following methods will be adopted to ensure full knowledge of the Policy:

- Newsbeat
- Intranet
- Posters
- Policy Portal

11. REVIEW.

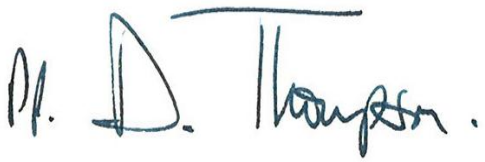
11.1. The policy business owner Information Management, maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

11.2. The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

11.3. A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted by the date shown as indicated on the first page.

11.4. Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

11.5. Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.



CHIEF CONSTABLE

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	11 Sept 2014	Initial Draft	Paul Richards – Information Security
0.2	11 Sept 2014	Amended Draft	Paul Richards/Stephen Laishley
0.2	12/09/2014	Amended formatting/completed missing parts	56408 Couchman
0.2	21/10/2014	Policy Published	56408 Couchman