DIGITAL ASSET MANAGEMENT SYSTEM (AETOPIA DAMS)

Owning Department: Specialist Operations Command

Department SPOC: DAMS Business Owner

Risk Rating: Medium Low

Legal Sign Off: 09.05.24

JNCC: 11.03.2024

Published Date: 17.04.2025 (V1.4)

Review Date: 12.03.2027

Index

Legal Basis

Legislation which you must check this document against (required by law)

- Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
- Equality Act 2010
- Crime and Disorder Act 1998
- Health and Safety at Work etc. Act 1974 and associated Regulations
- General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Freedom of Information Act 2000
- The Civil Contingencies Act 2004
- Criminal Justice and Immigration Act 2008
- Protection of Children Act 1978
- Criminal Justice Act 1988

Other documentation which you must check this document against:

- College of Policing – Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- College of Policing – Authorised Professional Practice
- Review, Retention and Disposal of Crime and Non-crime related information Schedule

1. Summary of Changes

1.1 This is a new joint policy: Digital Asset Management System (Aetopia DAMS).

2. Introduction

2.1 The Aetopia DAMS is the new Digital Asset Management System (DAMS) introduced across the 5 Force collaboration (Bedfordshire, Cambridgeshire, Hertfordshire, Norfolk and Suffolk) to store and manage all types of digital media for evidential purposes.

2.2 The Aetopia DAMS is provided as a cloud hosted Software as a Service (SaaS) managed service, accessed from force networks by way of an internet browser.

2.3 The system effectively replaces the DEMS 360 user interface where officers and staff historically accessed their Body Worn Video (BWV) footage, Digital Interview Recording (DIR) footage and uploaded miscellaneous pieces of digital media.

2.4 Body Worn Video footage and Digital Interview Recording footage is automatically uploaded into the Aetopia DAMS.

2.5 DAMS users are able to upload digital media from a force device or network location and to edit material.

2.6 DAMS users are able to share assets and cases with internal and external users and share links to the material with the Crown Prosecution Service (CPS).

2.7 Users are able to create email requests for members of the public and other external parties to upload media.

2.8 The system will be used by all officers and by staff from across the organisations.

3. Aims

3.1 This document provides officers and police staff with guidance for storing, managing and sharing digital media in the Aetopia DAMS.

3.2 The purpose of the policy is to ensure the Aetopia DAMS is used correctly so that Norfolk and Suffolk Constabularies gain maximum benefit from its operational use.

4. Statement of Policy

4.1 This policy has been formally agreed via the approved policy development/review process. It will be maintained by the Specialist Operations Command in conjunction with the Central Policy Unit.

4.2 The policy is intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status.

4.3 Managers have a responsibility to ensure this policy is applied fairly, and unless otherwise stated, all policies and procedures are non-contractual.

5. Applicability

5.1 This policy is aimed at all Norfolk and Suffolk Constabulary personnel who are authorised to use the 5 Force Aetopia DAMS, their supervisors and managers.

5.2 DAMS users, their supervisors and managers are expected to comply with this policy and training in its usage.

5.3 The DAMS solution and the data stored and managed in the DAMS is only to be utilised for policing purposes.

5.4 If officers / police staff do not use DAMS in accordance with this document, they may be held to account at a later stage.

6. Roles and Responsibilities

DAMS Management Roles	**Responsibilities**
DAMS Business Owner	Ensuring appropriate DAMS user representation at the 5Force Aetopia DAMS user working group. Maintenance of the DAMS Force Policy and Business Continuity plans. The Norfolk and Suffolk Role of Information Asset Owner (IAO) for DAMS. Representation of Norfolk and Suffolk on the 5Force DAMS Governance Group. Chair of the Norfolk and Suffolk DAMS Governance Group.
DAMS N/S Governance Group	Facilitating DAMS user change requests, future developments, reviews, and implementation. Monitoring and maintenance of user licence levels, including the following up of leavers from DAMS. Managing invoices for use of the DAMS. Monitoring DAMS storage levels. The control of the authorisation of users requesting system permissions for roles which cannot be given by direct link to their role, i.e.: Image Technicians or Professional Standards Department (PSD) Admins. Provision of business support for users. (See Business Support below)

Leads for: BWV; DIR; Other evidential digital assets including CCTV	Leads for; BWV; DIR; Other evidential digital assets including CCTV representation at the DAMS N/S Governance Group
Information Management	Information Management representation at the DAMS N/S Governance Group
PSD SPoC	PSD representation at the DAMS N/S Governance Group
TSU SPoC	Technical Support Unit (TSU) representation at the DAMS N/S Governance Group
CJS SPoC	Criminal Justice System (CJS) representation at the DAMS N/S Governance Group
CIU SPoC	Custody Investigation Unit (CIU) representation at the DAMS N/S Governance Group
JPSC SPoC	Joint Protective Services Command (JPSC) representation at the DAMS N/S Governance Group
Norfolk and Suffolk CPC SPoCs	Norfolk and Suffolk County Policing Command (CPC) representation at the DAMS N/S Governance Group
S&I (Norfolk) / I/CSIM (Suffolk) SPoCs	Safeguarding and Investigations (S&I) (Norfolk) / I/CSIM (Suffolk) representation at the DAMS N/S Governance Group
ICT Support SPoC	ICT Support representation at the DAMS N/S Governance Group
Finance SPoC	Finance representation at the DAMS N/S Governance Group
SBOS SPoC	SBOS representation at the DAMS N/S Governance Group
Service Desk	Responsible for the first line contact for users in technical support of the system
Applications Team	Responsible for second line support for users in technical support and liaison with the supplier

Business Support	<u>DAMS Data Administrator</u> Managing access to secure/closed assets and cases held in the Aetopia DAMS (excluding those that are restricted to PSD and ACU only). <u>DAMS PSD Data Administrator</u> Managing access to secure/closed assets and cases held in the Aetopia DAMS which are restricted to PSD and ACU <u>Digital Champions</u> First line peer business support for user queries in the use of the Aetopia DAMS
Records Retention and Deletion Team	Managing the review and retention of assets in the Aetopia DAMS including the deletion of assets where applicable.

7. Definitions

Term	**Definition**
Asset	All media files in the Aetopia DAMS
Case	Cases in the Aetopia DAMS are folders used to group all assets relating to an investigation together from where they can be viewed and managed as a group.
Closed assets/cases	Assets/cases where it is deemed necessary to hide the presence of the asset/case from other DAMS users. Access to the material is restricted to the asset/case owner and named individuals. Other DAMS users are not able to see any evidence that the asset/case even exists. Access to closed assets/cases is managed by DAMS Data Administrators.
Lightbox	A container for media files and cases that can be shared securely with other DAMS users or with external third parties.
Metabase	A reporting repository used for management reporting on the Aetopia DAMS activity and contents and provides a full audit history of that activity.
Sandbox	A quarantine area where third party uploads are virus checked and validated before being loaded into the Aetopia DAMS system.

Secure assets/cases	Assets/cases where it is deemed necessary to restrict access to the material held in the Aetopia DAMS to the asset/case owner and named individuals typically where the content is of a sensitive nature. Other users are able to see that an asset/case exists but is not able to access any of the content. Access to secure assets/cases is managed by DAMS Data Administrators.

8. User Access

8.1 All officers and selected staff roles will be automatically granted access to the Aetopia DAMS with access privileges based upon the individuals Department, Section, Unit and Team where possible.

8.2 There are scenarios where it is not possible to automatically grant access to an individual (e.g. a role cannot be automatically determined based upon a User's Department / Section / Unit / Team, an individual has more than one HR assignment record, etc.).

8.3 Where a user requires access to the Aetopia DAMS and access has not been automatically granted, access can be requested via the SailPoint Request Centre accessible from the DAMS Intranet page.

8.4 DAMS user access requests must be approved by the DAMS Business Support Team.

8.5 The DAMS user roles available are:

DAMS User Type
Standard User
Anti-Corruption Unit (ACU Officers and Staff only)
Audit (Information Management Staff only)
Image Technician (Provides access to Image Technician workflows - Criminal Justice Image Technicians only)
Image Technician Supervisor (Enables user to manage the Image Technician Workflow queue - Justice Image Technician Team Leaders only)
Professional Standards Dept (PSD Officers and Staff only)
Professional Standards Dept Data Admin (Enables users to provide access to SECURE/CLOSED assets/cases - Named PSD Officers and Staff only)

Records Retention and Deletion User (Enables the deletion of assets and case from DAMS - Information Management MOPI Team only)
Standard Data Admin (Can share and provide access to SECURE/CLOSED assets/cases with the exception of PSD/ACU restricted assets - Named individuals only)
Technical Support Unit (Provides ability to manage and work Technical Support workflows - TSU Team only)
Transcriber (Provides access to Transcription workflow - Criminal Justice Summarisers only)
Transcriber Supervisor (Enables user to manage Transcription workflow queue - Criminal Justice Summariser Team Leaders only)

9. Audit Trails

9.1 The Aetopia DAMS provides an audit trail for the last 30 days activity against assets, cases and lightbox shares.

9.2 A full audit of activity in the Aetopia DAMS is available separately in the Metabase reporting solution linked to the Aetopia DAMS.

9.3 Officers and staff that are assigned to the DAMS PSD, ACU, Audit and Business Support roles will be granted access to Metabase.

9.4 Where a user requires access to the Aetopia Metabase, and access has not been granted, access can be requested via the ICT Self Service Portal.

9.5 Metabase user access requests must be approved by the individual's line manager and approved by the DAMS Business Support.

10. Training

10.1 Before using the Aetopia DAMS, it is the user's responsibility to ensure they have completed the mandatory training packages.

10.2 The Aetopia DAMS training can be found on the LMS training system Best I Can Be (thebesticanbe.uk).

10.3 Users should also refer to this DAMS Force Policy for current guidance on how to use the DAMS.

11. Securing Assets

11.1 The securing of assets and cases is available to all users but should only be used where there is a genuine business need to restrict the access. If a user secures an asset or case, then they cannot un-secure it. This will need to be done by a Data Administrator.

11.2 Inspectors and certain members of the DAMS Business Support are Data Administrators. In the first instance, a request to remove the secure status from an asset/case should be made to DAMS support at DAMS.support@norfolk.police.uk. If the need is urgent and cannot wait, an Inspector should be contacted.

12. Storing Material on DAMS

12.1 The purpose of the DAMS is to store media files e.g. BWV, DIR, audio video files, still images and audio files.

12.2 Case documents should not be stored in the Aetopia DAMS. Case documents should be stored on the Athena Case Management system.

12.3 Exhibited or Unused 999 calls required to be shared with the CPS. A copy of the recording should be requested to be extracted from Redbox and uploaded into the Aetopia DAMS.

12.4 XRY files should not be stored in the Aetopia DAMS and should be stored in the central XRY repository.

12.5 Illegal images or video (extreme pornography or indecent images of children, as defined under s63 of the Criminal Justice and Immigration Act 2008, Protection of Children Act 1978 and s160 Criminal Justice Act 1988) must not be uploaded to or stored on the DAMS. Officers and staff who encounter material which may be illegal should secure it and contact the TSU as soon as practicable for advice. TSU should secure and remove the illegal data from the network where it would be passed to DFU for entry onto the secure DFU data centre.

12.6 If illegal material is discovered within the DAMS, the relevant assets must be secured, and contact made with TSU as soon as practicable for advice.

12.7 Explicit material which is not unlawful can be stored on the DAMS. The file name must include the words “EXPLICIT CONTENT”. Explicit material should not be shared with the CPS in the first instance. OICs should clearly describe the contents of the material in their case file submissions and only provide the material on receipt of a direct and reasonable request from the CPS to do so.

12.8 Such material should also be masked to stop potentially offensive material appearing as a thumbnail.

13. Data Retention and Management

13.1 It is the responsibility of officers / staff uploading assets into the Aetopia DAMS to categorise their assets with the correct evidential status (Evidential or Non-Evidential) and an associated offence code.

13.2 A combination of an assets’ evidential status and offence code determine an assets retention in accordance with the Constabularies’ Review, Retention and Disposal of Crime and Non-crime related information Schedule.

13.3 Non-evidential assets in the Aetopia DAMS will be deleted automatically after 31 days in-line with the force retention policy.

14. Editing DAMS Assets

14.1 DAMS provides the ability for users to edit images and audio video files. Users are encouraged to carry out basic editing of assets in the Aetopia DAMS in-line with the 5F DAMS business case. Complex editing must be performed by the Image Technician team and the Technical Support Unit.

14.2 Basic editing in the Aetopia DAMS is defined as:

- Editing still images by:
  - Cropping images,
  - Rotating images,
  - Blurring parts of an image.
- Creation of snapshots from audio video footage e.g. CCTV and BWV.
- Clipping audio video footage.
- Removing all audio from audio video footage.
- Basic blurring of audio video footage e.g. static images in audio video assets such as a parked car number plate, filmed on a static camera such as fixed CCTV camera, ring doorbell etc.

14.3 Complex editing is defined as:

- Partial audio redaction from audio video assets.
- All other blurring of audio video assets not specifically identified as basic editing above.
- Compilations / storyboarding of audio videos clips.

14.4 Requests for the partial removal of audio from audio video assets must be made using the Aetopia DAMS workflow “N/S Media Request Image Technicians” and must include timings of audio redactions.

14.5 Requests for blurring of moving subjects (e.g. faces / car indexes) must be tasked via DAMS workflow “N/S Media Request TSU”.

14.6 Requests for ‘story boarding’ (compiling different assets to create a single file, most commonly used to link different CCTV camera files to create a ‘movie’ of a single incident e.g. the movements of an offender through a shop) must be tasked via the Aetopia DAMS workflow “N/S Media Request Image Technicians”

15. Physical Media

15.1 Where media cannot be uploaded into the Aetopia DAMS and is obtained on physical media (e.g. Disk, USD Stick, etc), the physical media must be sent to Central Media Store.

15.2 The OIC must create a ‘Place Holder’ asset in the relevant Aetopia DAMS case and task the Image Technicians with the upload from physical media using the

Aetopia DAMS workflow “N/S Media Request Image Technicians”. The detail of the TranSearch Barcode number attributed to the physical asset must be included in the request notes.

16. Conversion of Unplayable Audio Video Assets

16.1 Where media files uploaded by third parties cannot be converted automatically into a playable form by the Aetopia DAMS, the OIC must task TSU to convert the media using the Aetopia DAMS workflow “N/S Media Request TSU”.

17. Transcribing Interviews

17.1 Requests to transcribe interviews must be made via the Aetopia DAMS N/S Transcription Request workflow.

17.2 The transcripts produced by the summarisers will be uploaded to the relevant cases in Athena.

18. Sharing Material with CPS

18.1 When sharing a link to media held in the Aetopia DAMS with the CPS, the user sharing the link must ensure the link copied on to the MG0 shows as a hyperlink and not as text. This is achieved by the user adding a space or carriage return after the copied text.

19. Sharing Material with Third Parties

19.1 It is possible to share DAMS assets with other agencies or individuals where deemed lawful and appropriate.

19.2 When sharing media held in the Aetopia DAMS, the expiry of the share defaults to 31 days. This should only be extended where there is a valid business need. Shares should never remain open longer than is absolutely necessary.

19.3 Where a defendant is representing themselves and needs to be supplied with case material, this must be completed by the OIC.

20. Data Breaches

20.1 If the case is at the pre-charge stage, the OIC of the case must report the breach immediately by completing Information Security Data Breach Recording Form and e-mailing it to InformationSecurity@suffolk.police.uk . It must be made clear on the form that the breach has occurred as a result of sharing with DAMS.

20.2 If the case is being managed by the CJU, the team receiving notification of the breach will contact the OIC to notify them of the breach and the requirement to complete a report to Information Security.

20.3 If the OIC is not on duty, the CJU will report the breach on their behalf and notify the relevant Inspector of any urgent actions required.

20.4 Any actions required resulting from the breach (risk assessments; notification of involved parties; retrieval / deletion of any disclosed data / media) must be detailed on the breach form and updates about progress provided to Information Security.

21. Leavers

21.1 Where a DAMS user leaves either Norfolk or Suffolk constabulary, irrespective of the reason, it is the responsibility of the leaver's immediate supervisor to ensure any Body Worn Video footage is uploaded from any BWV cameras the user has access to before the user leaves.

21.2 Where a DAMS user leaves either Norfolk or Suffolk constabulary, irrespective of the reason, it is the responsibility of the leaver's immediate supervisor to ensure the ownership in the Aetopia DAMS of cases and assets owned by the leaver are taken on by an active DAMS user.