Police, Fire and Crime Commissioner for Essex

Electronic Filing System Policy

Version Control	Version 4.0	November 2020
Reviewed by	D Horsman	November 2020
Owned By	D Horsman	November 2020
First Published	T Bateman	November 2012
Next Review Date	D Horsman	September 2023

Version history

Version Number	Date	Reason for review	Comments
1.0	November 2012		First publication
2.0	February 2016	Update	Inclusion of PAM system
3.0	September 2017	Update	Inclusion re hyperlinking documents on email
4.0	November 2020	Update	Inclusion of new file naming convention and structure.
5.0	March 2022	Update	No additions made
6.0	May 2024	Update	Updated to reflect the move to SharePoint.

Electronic Filing System Policy

Introduction

The records of the PFCC are its corporate memory and are necessary to ensure good corporate governance, accountability and legislative compliance, as well as to provide evidence of decisions and actions and inform future decision-making.

All records created during the course of the PFCC's work are the property of the PFCC and will be regulated in accordance with the Data Protection Act and subject to requests under the Freedom of Information Act.

As set out in the Records Retention and Disposal Policy the Commissioner undertakes to:

- Manage records according to this policy
- Comply with legal obligations and best practice that apply to the management of their records
- Keep records electronically where appropriate
- Ensure that information is not kept for longer than is necessary. Often, information-rich cumulative or summary records will be retained in the longer terms while more detailed, bulky but ephemeral records can and should be destroyed earlier
- Retain the minimum amount of information that they require to carry out their statutory functions
- Store records safely and efficiently, utilising appropriate storage methods at all points in their lifecycle and disposing of them appropriately when they are no longer required
- Safeguard records necessary for business continuity in the event of an emergency or disastrous occurrence
- Encourage effective access to and use of records as a source of corporate information
- Identify and make provision for the preservation of records of historical value

As most of our documents are stored electronically this policy sets out the approach to file management and file storage and is an important aspect of our overall document management approach. This will ensure that the Commissioner and their staff are able to fully comply with their legal obligations under the Freedom of Information Act, the General Data Protection Regulation (GDPR) and Data Protection Act 2018 while also following the wider policy framework in particular the Records Retention and Disposal Policy and Data Protection Policy.

File naming

When saving any documents on the shared drive or distributing for comment a standard name format should be used. This will make it easier to find, search and access documents and provides a shared way of tracking different versions of a document. For simplicity a similar file naming system to that of Essex Police is to be used:

YYYYMMDD Title Type Version
(Colouring is only used for the explanation in this guide and not for actual file naming)

YYYYMMDD – date format complies with ISO and maintains chronological order within a file
Title – the title should match the title of the document where possible
Type – strategy, report, agenda etc
Version – drafts should start with a 0 i.e. V0.1. Final documents should start with a 1 i.e. V1.0. Draft revisions to a previously approved document would have both an 'approved number' (before decimal point) and a draft number (after the decimal point).

Eg. **20200228 HMICFRS FRS Inspection Report V1.0**
20191123 Draft PFCC Risk Register Letter V0.3
20200302 ECJB Terms of Reference TOR V2.1

Folder creation

To prevent the office's SharePoint sit becoming oversized and disorganised any new Team created must fit within the thematic organising logic currently used. These top Team levels are locked and any new Teams require agreement from the Senior Information Risk Officer. When considering whether a new folder is required it must first be checked that a similar folder doesn't already exist. A new folder may be created only if a document cannot be appropriately filed within an existing folder.

File review

Files should be reviewed in line with Data Asset Register and File Retention Schedule at least every 6 months. Duplicate documents, or information no longer required, (e.g. availability for past meetings) should be deleted. Compliance with this is dip sampled by the DPO on a quarterly basis.

When reviewing stored documents, the following principles of records management should be followed:

- Legislation or statutory requirements requiring a document to be kept
- Accountability – document containing legally required information (past or present)
- Business purpose – e.g. audit trail
- Historic value – research or background material of possible value

If you are unclear about whether a document should be stored or deleted first check the record retention schedule. If you need further guidance please discuss your issue with the Data Protection Officer.

PAM Correspondence system

PAM is an independent document management system. Correspondence, telephone calls and information to be monitored can be recorded on PAM.

Documents recorded on the PAM system and will be given a reference number / year (eg.1234 2016).

Any correspondence /information will also be saved in the office shared drive within the correspondence folder.

The original correspondence will therefore be recorded as per following example:

1234 2016 Surname of Correspondent date received e.g. 1234 2016 Smith 15.02.16

Followed by R for response or A for Acknowledgement e.g. 1234 2016R Smith 15.02.16

Further correspondence will be listed as 1234 2016F and further response FR etc.

Once recorded in the Shared Drive they can be saved on the PAM log.

Data Protection

Data Protection is all our responsibilities and how we store, protect and manage our documents is fundamental to how we manage our data. Our obligations as staff and how we will manage data within the office is clear set out within the Data Protection Policy.