AVON & SOMERSET POLICE & CRIME COMMISSIONER

Information Governance Guidance for staff

Version 1.0 February 2019

Information Governance in the Office of the Police and Crime Commissioner (OPCC) covers the business areas;

- Information Security,
- Data Protection,
- Records Management and
- Freedom of Information.

This guide is intended to provide all employees with the minimum expected standards and knowledge to achieve a good level of compliance across the organisation.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Information Security

- Physical Security

Everyone is required to carry and display Identification on all Avon and Somerset Constabulary sites.

All staff have a responsibility to challenge persons who are within police sites and who are not displaying identification. If they are not satisfied, the person will be required to leave or return to the reception point.

Lost or stolen cards must be reported immediately to service desk

- Email

There is no expectation of privacy, the email system is monitored.

Suspicious email – don't click on a link, attachments or reply to the email, seek advice from the Service Desk.

Send all emails containing personal data to a secure email address (PNN, CJSM, CGSX) and mark the email appropriately under the GSC.

- Passwords

Use a mixture of letters, numbers and symbols to strengthen the password.

Do not share your passwords or write them down.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Information Security continued

- Confidential disposal

Identify the location of your secure waste bins /Limit printing hardcopies of data.

- Lock your screen when away from the computer and use privacy screens on laptops.

- Removable media

Do not connect any external device to the network without approval of #servicedesk.

- Social networks

Do not identify yourself as a police employee.

- Clear desk policy.

- Keep all equipment appropriately stored, don't leave equipment 'on show' in cars.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Data Protection

- Force systems should only be accessed for an OPCC business/policing purpose e.g. to do with your role in the OPCC. ‘Intelligence checking’ is not permitted.
- All force systems are audited to ensure compliance.
- Double check all email recipients and postal addresses to confirm they are correct prior to sending data.
- Blind carbon copy – if sending an email to more than one external recipient ensure you use the BCC functionality.
- Information Sharing with external partners must be:

J – Justified, A – Appropriate, P – Proportionate, A- Auditable, and N- Necessary.

- Ensure third party personal data is redacted (blacked out) appropriately prior to release, using specific software designed for this purpose where possible.
- Do not discuss OPCC business/police intelligence etc. outside of the workplace.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Data Protection – Data subject rights

There are several rights under Data Protection Legislation, however these are those which are the most relevant to OPCC employees.

- Right of access:

Individuals have the right to access their personal data and supplementary information, subject to certain restrictions. The subject access process must be completed within one calendar month by the Contacts team, don't delay sending requests from members of the public through to them.

- Right to rectification:

You must rectify inaccurate personal data when it becomes apparent, or, if an individual requests it. All requests must be sent to the Data Controller (OPCC CEO).

- Right to erasure:

Individuals also have the right to request the deletion or removal of their personal data. Requests relating to the erasure of locally held information on OPCC systems needs to be directed to the Data Controller (OPCC CEO).

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Data Breach or Security Incident

A personal **data breach means** a **breach** of **security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal **data**. This includes **breaches** that are the result of both accidental and deliberate causes.

Examples of Data Breaches/Security Incidents:

- Sending an email to an insecure email address.
- Failure to redact information
- Accessing the systems for a non policing purpose.
- Failing to use the BCC functionality on an email.

A Data Breach or Security Incident can be very costly for an organisation both in levels of fines and damage to our reputation.

If a Breach or Incident occurs follow the Breach of Data Protection policy and advise the Data Controller or Contacts and Conduct Policy Officer immediately.

..\..\..\OPCC Policies and Procedures\HR Policy and Procedures Handbook\OPCC\OPCC Breach of Data Protection GDPR - internal Policy May 18.doc

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Government Security Classification

OFFICIAL

Documents only need to be marked OFFICIAL when:

- OFFICIAL Organisation / performance.
- OFFICIAL Management information.
- OFFICIAL Personal information.
- OFFICIAL Business information.

NO MARKING REQUIRED

There is no need to mark every document.

Only mark a document if it falls within the OFFICIAL or OFFICIAL-SENSITIVE categories

HANDLING INSTRUCTIONS

To enforce the need to know principle handing instructions can be placed on any document, however **must** be present on OFFICIAL – SENSITIVE..

Handling instructions are to provide additional measures on how you want the recipient/s to manage the document or email you have shared and the instruction should consider the following:

- Who can see or have access to the information?
- What are they allowed to do with this information?
- What they need to do to ensure it is kept secure and how to dispose of it.

OFFICIAL – SENSITIVE

When to apply the OFFICIAL - SENSITIVE caveat:

- OFFICIAL-SENSITIVE Cause a risk to life and/or safety
- OFFICIAL-SENSITIVE Have an impact on security or intelligence led operations.
- OFFICIAL-SENSITIVE Be breaching legislation (DPA)
- OFFICIAL-SENSITIVE Detrimental Impact on an investigation.

OFFICIAL SENSITIVE should be used where there is a clear and justifiable requirement to reinforce the ‘need to know’ principle and carries a higher level of risk and could have severely damaging consequences if compromised.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Records Management

All OPCC and Avon and Somerset Police information should be held in accordance with the Records Retention Policy.

For the purposes of this guidance the term " Data Quality" is defined as data which is fit for the intended purpose and is 'Accurate, Adequate, Relevant, and Timely':

- **Accurate –** Care must be taken when recording information and where appropriate the source of the information must also be recorded. If there is any doubt over the authenticity of the information clarification must be sought from the source.
- **Adequate –** Recorded information must be accurate and sufficient for the policing purpose in which it is processed. All recorded information must be easily understood by others.
- **Relevant –** Recorded information must be relevant to the policing purpose. Opinion needs to be clearly distinguished from the facts.
- **Timely –** Information must be promptly recorded into the relevant business area in accordance with the agreed timescales.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Freedom of Information Act 2000

The Freedom of Information Act 2000 gives a general right of access to all types of **recorded information held by public authorities** which includes the OPCC.

Any individual can make a FOI request to us, however it must be:

- Made in writing,
- Include the requesters name and an address for correspondence (either email or postal address) and
- Describe the information being requested.

There is no fee involved in making a FOI request.

There is no obligation for the OPCC to create information in order to answer to questions.

A request may be received anywhere within the OPCC and the 20 working day timeframe for a response starts the day it is received.

- If you receive a request that mentions FOI or a request for recorded information held by the OPCC, this needs to forwarded promptly to the Contacts team.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

Useful links

- Mandated NCALT Packages:

Managing Information – Non operational.

Government Security Classification.

- The Centre for the Protection of National Infrastructure animations – It's ok to say, Spear Phishing – Don't take the bait.

- Pocketbook – Relevant Information Governance Policies.

AVON & SOMERSET POLICE & CRIME COMMISSIONER