

## OPCC Information Management Strategy

### Document Approval and Identification

Author	Michael RICHMOND
Version Number	1.1
Date	22 <sup>nd</sup> January 2020

### Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
1.0	1/10/2018	Mike Richmond	Rachel Cook	
1.1	22/1/2020	Mike Richmond	Mike Richmond	Transfer to new template

### WHO IS THIS STRATEGY FOR?

All employees of the Office of the Police and Crime Commissioner for Humberside need information every day in order to do their jobs. This strategy is for all our staff and it outlines what we need to do to manage our information better.

### WHY DO WE NEED A STRATEGY?

Information comes in many forms and is held in a variety of printed and electronic formats. We use this information in our daily working lives for many reasons including delivering services, formulating policy, holding meetings and managing staff. To maximise the potential benefit from our information we need to manage it effectively, re-use it where we can, share it appropriately and ensure that it is adequately protected.

### KEY PRINCIPLES

- sharing and re-using information using systems and technology;
- joining-up information flows and processes;
- exploiting and enabling the re-use of information;
- compliance with legislation and regulations.

### WHAT DOES GOOD INFORMATION MANAGEMENT LOOK LIKE?

Every member of staff in the Office of the Police and Crime Commissioner can say:

*'I know what information we've got and where it's stored'*

*'I collaborate with others to share knowledge and information'*

*'I know how to protect information and manage it appropriately'*

*'I have the skills I need to manage information'*

*'I know what's expected of me when creating and using information'*

*'I am part of an organisation which values knowledge and information'*

*'I know what information we've got and where it's stored'*

Providing staff with the right tools for managing information and training them in their use will help everyone to know what information is available to them, why it's being held and where it's stored.

**We will:**

- reduce the volume of information that we hold, only keeping information where there is a business need to do so, and in line with statutory requirements, such as the Data Protection Act 2018 (DPA);
- increase staff awareness of the information that they create, e.g. by avoiding unnecessary emails and re-using information to avoid duplication;
- promote the use of shared corporate repositories;
- maintain our knowledge of the information held by the organisation through use of an Information Asset Register (IAR);
- securely dispose of information when we no longer require it;
- work to identify vital records and ensure they are managed effectively;
- find effective solutions for managing our paper records as well as our electronic information.

**'I collaborate with others to share knowledge and information'**

Information and knowledge are key corporate assets and we all have a responsibility to share and re-use them to release their value and maximise benefits to the business and the public. Data held by the organisation should be open to re-use unless there is a good reason not to.

**We will advocate:**

- a risk-based approach to sharing to ensure information and knowledge are shared responsibly;
- the sharing and re-use of information to meet the business need;

- sharing of appropriate information with the public to meet our commitments on transparency and accountability, and facilitating the re-use of data to increase economic and social value.

**We will:**

- maintain common data sharing principles and agreements;
- maintain a clear picture of who we need to share information with and manage this in a responsible way;
- develop a clear picture of where information and knowledge resides across the organisation

**‘I know how to protect information and manage it appropriately’**

We will work to achieve an environment where staff are risk aware and have the confidence to share information. Whilst ensuring that information is properly protected, we will appropriately and effectively share information in order to protect and inform the public.

**We will:**

- Comply with the Data Protection Act (2018) and create policies that enshrine its principles into our working practices;
- adopt the Humberside Police Information Security Policy, ensuring that procedures for handling breaches are strictly adhered to, and lessons learnt are incorporated into ways of working;
- explore secure ways of working with new technologies, such as social media and collaborative work spaces, ensuring that staff are informed about their responsibilities when using them, both at work and at home, and are held to account;
- build information requirements into our business continuity procedures, by identifying those information assets which are business critical and protecting them accordingly;
- ensure that each information asset has an Information Asset Owner (IAO);
- ensure ongoing access and usability of information through and after data migration and business change;

**‘I have the skills I need to manage information’**

We will ensure that all staff have the knowledge, skills and support they need to manage information and use it appropriately.

**We will:**

- ensure that IM awareness is reflected in our induction training and development of everyone in the OPCC throughout their career;
- ensure that staff have the skills to use new technology, such as collaboration tools, to their maximum potential;

- ensure that staff are aware of the handling requirements for personal and special category data.
- ensure that staff know who to contact when they require advice or guidance on IM and ensure that help is readily available by appointing a Data Protection Officer who reports directly to the CEO.
- encourage staff to consult and involve experts early when managing specific types of information so that it is used and handled appropriately.

### **‘I know what’s expected of me when creating and using information’**

We will ensure that staff know what is expected of them when creating and using information through IM Policies and guidance:

#### **We will:**

- ensure IM policies and guidance are easily accessible and kept up to date;
- ensure our policies and working practices reflect our changing business and make full use of our IT systems;
- proactively disseminate IM policies, promoting awareness and ensuring they are followed.

#### **Through regular training and communication we will ensure that staff:**

- know why managing information properly is crucial;
- know that they have a personal responsibility to manage information-related risk;
- have the confidence to use and share information.

### **‘I am part of an organisation which values knowledge and information’**

We will develop an organisational culture which values information and works to remove barriers to managing information effectively. We will communicate our vision and culture to all staff and stakeholders.

#### **We will:**

- value the sharing of information and knowledge and recognise the consequences of not sharing;
- give staff confidence and trust in the quality of our information
- value protecting information appropriately;
- make it clear that good IM is everyone’s responsibility and part of how people do their jobs every day;
- view managing information as an enabler to our business and not an additional responsibility;
- work proactively and not just react when things go wrong;
- encourage collaborative working and discourage silo working;

- value corporate benefits over individual benefits thus encouraging the retention of knowledge within the organisation.

## **Appendix A: Information Management Policy Structure**

### **Data Protection**

We will maintain a **Data Protection Policy** for the OPCC.

### **Information Security**

The OPCC will adopt Humberside Police's **Information Security Policy**.

### **Records Management**

The OPCC will develop a **Records Management Policy** including a Review, Retention and Disposal schedule.

### **Freedom of Information**

The OPCC will maintain a **Freedom of Information Policy**