

By: Stuart Beaumont, Head of Community Safety and Emergency Planning

To: Kent Community Safety Partnership – 17 October 2013

Classification: For information

Subject: Information governance and its implications on Community Safety

Summary: This report reviews the changes occurring within the information governance environment and its implications on Community Safety.

1.0 Background

- 1.1. The Data Protection Act 1998 (DPA) defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Although the Act itself does not mention privacy, it was enacted to bring UK law into line with the EU Data Protection Directive of 1995 which required Member States to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. In practice it provides a way for individuals to control information about themselves.
- 1.2. Nationally, the Information Commissioner's Office (ICO) is the UK's independent public authority set up to uphold information rights. They do this by promoting good practice, ruling on complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken.

2.0 Increasing importance of information governance

- 2.1. One of the risks with information sharing is that of the data being lost or finding its way into the public domain. The risk of a serious data breach is one which now incurs a harsh financial penalty. The ICO, which has the power to issue monetary penalties of up to £500,000 in response to serious breaches of the Data Protection Act, has since January 2012 issued penalties totaling over £2 million to organisations who form the membership of Community Safety Partnerships. The largest fine to be issued so far was to the Brighton and Sussex University Hospitals NHS Foundation Trust for £325,000 for the improper destruction of computer hardware and subsequent breach of sensitive data.
- 2.2. Within Kent, organisations are working to protect themselves against breaches by enacting policies and technology to tighten up their information sharing arrangements. The main partnership agreement to help facilitate this is the Kent and Medway Information Sharing Agreement, which was created to provide a multi agency data sharing protocol for public and private organisations and currently has approximately 70 signatories. The agreement is administered by the Information Governance Programme Board, which oversees and ensures effective implementation of information sharing arrangements.

- 2.3. Furthermore, the legislative situation will change as the European Commission is currently drafting a new Data Protection Directive which is expected to be introduced in 2013. The draft directive is expected to be introduced as a regulation, which will apply directly to all EU member states including the UK. The new directive will introduce several elements including: the 'right to be forgotten' (allowing the public to request an organisation to destroy all data pertaining to them); the principle of 'data portability' (allowing the transfer of personal data between service providers); and the toughening up on the need for 'direct' consent.

3.0 Government Protective Marking Scheme

- 3.1. Nationally, to assist with ensuring appropriate information security standards, HM Government has a protective marking scheme for sensitive documents which has been in active operation for nearly a century. The current operational scheme employs five markings, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET, & TOP SECRET. The markings relate to the level of risk applicable if the information were made public.
- 3.2. This scheme is soon to be revised which will see the reclassification of the existing markings. In the new scheme PROTECT, RESTRICTED and CONFIDENTIAL will be merged into the one marking titled OFFICIAL. The new scheme has already been adopted by KCC, with a protective marking policy about to be rolled out which will see the use of OFFICIAL along with a descriptor which will identify the information's 'impact level' (level of risk). Central Government is expected to officially launch the new scheme during late 2013 and it is likely to take several years to become fully operational.
- 3.3. The new scheme may challenge existing data sharing arrangements involving partners who are strict operators of the existing model and may be reluctant to change to the new combined marking. As a result staff will need to be briefed on both schemes in order to work effectively until all agencies transfer to the new scheme.

4.0 Current situation

- 4.1. Community Safety Units are both authors and handlers of sensitive 'RESTRICTED' level data and have a business need to integrate information security policies and procedures. This includes Domestic Homicide Reviews, Strategic Assessments, and sensitive personal data, to name a few.
- 4.2. A variety of secure email systems have been introduced to allow for secure communication and transfer of sensitive data for the purposes of DHRs. CJSM and GCSX accounts have been provided for partner level communication, whilst Egress is currently being rolled out to enable communication with external organisations without secure email. All of these systems allow for the safe and secure transfer of RESTRICTED level data.
- 4.3. Where sensitive data has been saved onto computer systems for later retrieval, specific folders have been restricted to certain users to ensure confidentiality.

- 4.4. Where hard copies of sensitive data exist they are locked away in secure cabinets in their respective locations.

5.0 Next steps

- 5.1 Partner organisations may wish to review all current work streams and identify those where it can be shown that there is the storing or processing of personal or sensitive data. Where personal or sensitive data is handled the appropriate measures will need to be put into place to ensure correct handling, storage, and destruction procedures take place in accordance with the Data Protection Act and related legislation.
- 5.2 A new set of guidance documentation is being prepared to provide knowledge and understanding to front line and back office staff about information sharing. Once completed and approved the guidance shall be disseminated to all staff and training needs identified to assist in its understanding.

6.0 Recommendations

- 6.1 The Kent Community Safety Partnership to note.