Creating a safer
Cambridgeshire

To: Business Coordination Board

From: Chief Constable

Date: 30 March 2016

PRIVACY COMPLIANCE

1. Purpose

1.1 The purpose of this paper is to update the Business Coordination Board ("the Board") in relation to Cambridgeshire Constabulary (the Constabulary's) Strategy and Policy to meet individuals' expectations of privacy in a lawful and proportionate manner. The paper covers surveillance, and how the 'Information Commissioner's Code on Conducting Privacy Impact Assessments' is used, as well as the Constabulary's compliance with its data protection obligations.

2. Recommendation

2.1 The Board is invited to note the contents of the report.

3. Background

3.1 The right of an individual to privacy is contained within the Data Protection Act (DPA) and the Human Rights Act (HRA), notably Article 8 which refers to the right to respect of his or her private and family life, their home and their correspondence. These rights are subject to proportionate and lawful restrictions.

3.2 Within the DPA there are 8 Data Protection Principles or obligations with which data controllers must comply when processing personal data. These are:

1. Shall be processed fairly and lawfully
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with these purposes
3. Shall be adequate, relevant and not excessive in relation to these purposes

4. Shall be accurate and where necessary kept up to date.
5. Shall not be retained for longer than is necessary for these purposes.
6. Shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to personal data
8. Shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.3 Principle 6 relates to the rights of individuals in relation to processing of personal data, which include:

1. Right of access. Subject to some exemptions, individuals have the right to be provided with a copy of any personal data held about them in any form; this is known as their Subject Access Right.
2. Prevention of processing likely to cause damage or distress.
3. Rectification, blocking, erasure and destruction.
4. Complaints to the (Information) Commissioner.

3.4 Within Cambridgeshire Constabulary, these rights are managed through the Information Management Department and the processes for doing so are published on the Constabulary website. The website also provides a Fair Processing Notice, informing members of the public what data we collect, the purpose for which it was collected and how it is used. A copy of this notice is also provided, along with complaint rights, in response to requests under the Subject Access provisions.

3.5 Sitting alongside the DPA is the Privacy in Electronic Communications Regulations 2009 (PECR), which give specific rights in relation to electronic communications. They are derived from European law and implement European Directive 2002/58/EC, also known as 'the e-privacy Directive'.

3.6 The e-privacy Directive complements the existing data protection regime and sets out more-specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.

3.7 Service providers must take appropriate measures to safeguard the security of their service. What 'appropriate' means depends on the nature of the risk, the technology available, and the cost. Service providers must also inform their customers of any significant security risks.

3.8 Whilst the Constabulary is not a Service Provider in the context of Skype, awareness of PECR does allow us to make better informed decisions around privacy issues in using the technology.

3.9 In addition to the above Acts, there are Codes of Practice issued by the Information Commissioner (ICO) which outline the best practices which should be considered by organisations which process personal information in order to assist them in meeting

their legal obligations under the Acts. These include Codes of Practice on: Data Sharing; CCTV; Anonymisation and Privacy Impact Assessments. None of these are mandatory.

3.10 Covert surveillance activities are regulated by the Regulation of Investigative Powers Act 2000 (RIPA).

4. Physical and Informational Security in Policing

4.1 'Physical' privacy is taken to mean the right of an individual to go about their daily lives without being impeded. Thus a person may not have their privacy impeded without there being a lawful purpose for doing so. CCTV may be considered to be an area where the physical privacy of an individual is encroached; and therefore where CCTV is in operation, there is an imperative to ensure that any encroachment is justified, minimised and use of images must be for the purposes for which they were originally obtained. Where an alternative could be used, that alternative should be the first consideration.

4.2 'Informational' privacy refers to the information which is held by the Constabulary in respect of individuals. The information which the Constabulary collects, and the purposes for which it is legitimately held, is also shown in our Fair Processing Notice (FPN). The FPN sets out the classes of information it holds; its reasons for doing so and how that information is handled. It is published on our external website and is monitored by the Force Information Manager.

4.3 An individual has the right (under section 7 of the DPA) to request a copy of the personal information which is held about them on our systems in whatever form. A copy of this information must be supplied to the individual within 40 calendar days of receiving a valid request, this is known as the Right of Subject Access and the process is shown on our website along with the relevant forms and instructions. In addition to this right, the individual has a right under Section 10 to prevent the Constabulary from processing any information which that person can demonstrate would cause them unnecessary alarm or distress. Finally, the individual has a right to have inaccurate or misleading information corrected or deleted from our records.

4.4 Within the policing context, the rights under Article 8 HRA are engaged within both 'physical' and 'informational' aspects.

5. Constabulary Governance Arrangements around Privacy

5.1 The Constabulary is subject to the Bedfordshire Police, Cambridgeshire Constabulary and Hertfordshire Constabulary (BCH) Information Management Policy and attendant procedures in relation to its strategies on data protection. In addition, we are also subject to the BCH Privacy Impact Assessment Policy and Procedures. These policies are based upon the College of Policing Approved Professional Practice; Code of Ethics; Data Protection and Human Rights Acts.

5.2 A Tri-Force "Information Charter" has been agreed by the three forces and is to be published prominently on each website. Overall responsibility for compliance lies with the Senior Information Risk Owner of each force and is enforced by the Force Data Protection Officer.

5.3 In Cambridgeshire the Senior Information Risk Owner is the Head of BCH Information and Communications Technology.

5.4 In October 2015, the Constabulary began to review its policies and processes in respect of Information Sharing, and seconded a specialist member of our Information Management Department to undertake that review. Once the review has been completed our external website will be fully updated to provide links to each policy; Information Sharing Agreement and associated Privacy Impact Assessment (PIA). Old policies have been removed and a notice advising of this intent to publish has replaced them. These documents will subsequently be reviewed on a rotational basis of not more than 2 years, whilst Fair Processing Notices are reviewed every 12 months (September), at the same time our annual notification is submitted to the Information Commissioner.

5.5 The Policy Review is expected to be fully completed by March 2016, with publication of Policies and completed PIAs available via our website with effect from April. Information Sharing Agreements will also be published externally where appropriate to do so and all documents are also subject to the requirements of the Freedom of Information Act.

5.6 In December 2015, a Tri-Force Information Management Lead was appointed, who will act as senior adviser to the forces.

5.7 Constabulary Information Assurance is managed by the Hertfordshire Information Assurance Officer and the Force Information Access Supervisor/Data Protection Officer. In the ICO PIA Code of Practice, the ICO suggests that the monitoring of PIAs would naturally sit with the DPO, who should be consulted at the earliest stage in the development of new projects.

5.8 Data Controllers must not process personal information without first registering with the Information Commissioner, unless exempt from registration. Cambridgeshire Constabulary is a registered body and subject to annual notification to the ICO in September of each year. Our registration is currently up to date and complete.

5.9 Since the introduction of the Tri-Force Privacy Impact Assessment (PIA) Policy, all new projects are required to undergo a PIA at inception, or as soon as the requirement to do so is identified. It is the responsibility of the Project Manager to ensure the PIA is completed in consultation with the DPO. External and/or internal consultation with relevant experts in any given area is permissible within the confines of the BCH Policy.

5.10 The preferred process is to involve the IMD during the earliest stages of a new project in order to fully advise on all aspects of privacy and informational risk assessment. At this point consideration should also be given to the creation of relevant policies, procedures, and cross-border agreements.

6. Individual Expectations on Privacy from the Constabulary

6.1 The Fair Processing Notice is published on our external website and, in addition, a copy of our notification to the Information Commissioner is available via their website. These documents clearly set out the types of information we hold, who (if anyone) we share that information and the purposes for doing so. It also describes who the Data Controller is and their contact details.

6.2 Our website also carries the contact details of our Data Protection Officer and the methods by which the Information Management Department can be contacted by mail, telephone or email. It also provides information as to how to apply for personal information held locally and/or the Police National Computer; how to request incorrect information to be amended or delete; and how to request that the individual may exercise their right to prevent processing where they believe it will cause them.

6.3 The use of an effective PIA is fundamental to the planning of any new project or revised process since it provides an opportunity to identify the most effective way for the Constabulary to comply with its data protection obligations and meet the privacy expectations of individuals in respect of their personal data. From a Constabulary perspective this helps reduce both the reputational risk as well as the potential financial consequence (the ICO has had the power to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act) should a significant privacy breach occur.

6.4 By publishing completed PIAs, we will improve the public confidence in the way in which we handle their information and demonstrate transparency, accountability through providing them with the knowledge of how and why we collect and use their information. We also provide them with a clear method of contacting us with any concerns which might arise as a result of our use of their personal information and how to resolve those issues.

6.5 Every computer in the Force is keystroke monitored and any breaches of data protection reported bank to the appropriate Governance boards. Each system search is covered by the Data Protection Act and only carried out for a lawful Purpose.

6.6 The Constabulary complies with the National Policy for ANPR Use, and is also compliant with current policies in relation to the use of Covert Surveillance and the requirements of RIPA.

7. Recommendation

7.1 The Board is invited to note the contents of the report.

BIBLIOGRAPHY

Source Documents	*Information Commissioner's Code on Conducting Privacy Impact Assessment* https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf *Cambridgeshire Constabulary – Data Protection Information* http://www.cambs-police.co.uk/about/dataprotection/
Contact Officer	Chief Inspector Andrew Bartlett, Information Management Department, Cambridgeshire Constabulary