REPORT TO: **STRATEGIC SCRUTINY MEETING**

DATE: **5 January 2017**

AGENDA ITEM: 7

SUBJECT: LANCASHIRE CONSTABULARY INFORMATION GOVERNANCE ANNUAL REPORT 2016

The purpose of this report is to provide the Commissioner with an overview of the Constabulary's performance and progress in relation to information governance in 2016.

INFORMATION GOVERNANCE

The Constabulary's Information Governance Board, chaired by the Senior Information Risk Owner, oversees and considers Information Governance issues for Lancashire Constabulary.

The Board provides the high level oversight, strategic direction, and leadership within the Force seeking to maximise the benefits of operational information in order to support effective decision making and to ensure the safe and lawful use of police information.

The Board oversees Force compliance with its statutory obligations, including those arising from but not limited to: -

- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2013
- Human Rights Act 1998

The Board also seeks to ensure compliance with national guidance such as the Management of Police Information (MOPI) guidance and NPCC Community Security Policy.

The Constabulary's central 'Information Governance function' sits within the Professional Standards Department.

DATA PROTECTION

Lancashire Constabulary is required to comply with the Data Protection Act 1998. The Act provides a detailed and complex regime for the protection of personal data of individuals. It sets out the rules with which organisations must comply when they obtain and use information they hold about individuals and it also gives certain rights to those individuals.

As a police force, Lancashire Constabulary holds and processes vast amounts of information relating to individuals and it is essential that this information is managed effectively to prevent and detect crime, not only to comply with the legislation. Detail of the purposes for which this information is collected and how it might be used is set out within its notification to the Information Commissioner, who is the UK Regulator.

There are a number of activities that the Force seeks to undertake in order to help ensure compliance with its obligations under the Data Protection Act, such as :

Data Protection Audits
Privacy Impact Assessments, prior to establishing new systems or initiatives which might include the processing of personal data
Creation of Information Sharing Agreements when information is shared with partner agencies on a regular basis
Provision of training to staff regarding compliance with the Data Protection Act.

Amongst other rights provided to individuals the Data Protection Act provides persons with a right to obtain information which might be held about themselves. Where an individual makes a request for information that might be held on the Police National Computer, the applicant will make the request to the National Criminal Record Office who will facilitate the disclosure on behalf of the Chief Constable. Otherwise, requests for local information will be processed by Lancashire Constabulary.

The table below sets out details of the number of local requests received by Lancashire Constabulary over the past three years:

Year	**2014**	**2015**	**2016 (up to 30 Sept)**
Requests received	264	260	259
ICO SA Complaints	2	4	8

The number of requests received to date in 2016 indicates that the year-end figure will show an increase of approximately 20% on the previous year. Within this figure there has also been an increase in the number of complex requests which require extensive material to be located and reviewed.

In 2016 the Constabulary has responded to the Information Commissioner concerning eight complaints in relation to responses provided to subject access requests.

Data Protection Act Breaches

Within 2016 seven data protection breaches have been recorded by the Force Information Assurance Manager, as Force Data Protection Officer. Following investigation and review of the circumstances in relation to these incidents none of these breaches were deemed serious enough to have been reported to the Information Commissioner. In some instances the Information Commissioner has been made aware of the breaches by the subjects concerned. In 2018 it will become a requirement for data protection breaches to be

reported to the Information Commissioner within 72 hours under the new General Data Protection Regulation.

The General Data Protection Regulation

The new EU General Data Protection Regulation (GDPR) will take effect from May 2018.

There will be a number of implications for the Force in terms of its obligations arising from this new legislation. The Regulation however applies to the processing of personal data for non-policing purposes, eg HR, finance, procurement. There is a European Directive which will need to be incorporated within domestic legislation that will apply to operational policing information for cross border transfers. Presently, there are no provisions to replicate the Regulations or Directive for domestic operational policing information, for which new legislation will be required. Potentially, a complex area of law will become even more complex for the Police Service.

It is clear that there will be corporate implications and also for the working practices of the Information Compliance Team. During 2017 the Constabulary will continue to plan for the new regulatory regime on the basis of the content of the Regulation, taking account of the guidance which will emerge from the Department of Culture Media and Sport and the Information Commissioner.

Information Disclosure

The Constabulary also considers the disclosure of police information for a number of other purposes, which take account of the requirements of the Data Protection Act, Human Rights Act and other relevant legislation. Where such disclosures are undertaken on a regular basis, this is usually in accordance with established procedures that seek to ensure that disclosures are necessary, proportionate and made in a secure manner.

Such disclosures include, for example, the disclosure of locally held information for the purposes of Disclosure and Barring Service checks, information in relation to insurance claims, information for civil litigation purposes and information for the proceedings before the family court. Where appropriate, in some circumstances the Force does seek to recover reasonable costs in accordance with NPCC Guidance.

The Disclosure and Barring Service (DBS) is an executive agency of the Home Office and the Constabulary receives funding for the resources which are required to manage and facilitate disclosure of local information where individuals are seeking to engage in roles working with or supporting children or vulnerable adults. In the past 12 months, 96,000 checks have been processed by the DBS team.

Demand in 2016 for the disclosure of police information for civil purposes and family court proceedings (997 requests in 2015) continues to grow and has increased in 2016 to date by approximately 10%. It is forecast that demand will continue to grow in relation to family court disclosure requests in 2017.

FREEDOM OF INFORMATION

The Freedom of Information Act 2000 was fully implemented on 1 January 2005 (various sections were brought into force in stages before this date). The Freedom of Information Act provides a right of access to information held by public bodies and is intended to be mutually exclusive to the Data Protection Act. So, if an individual requests access to

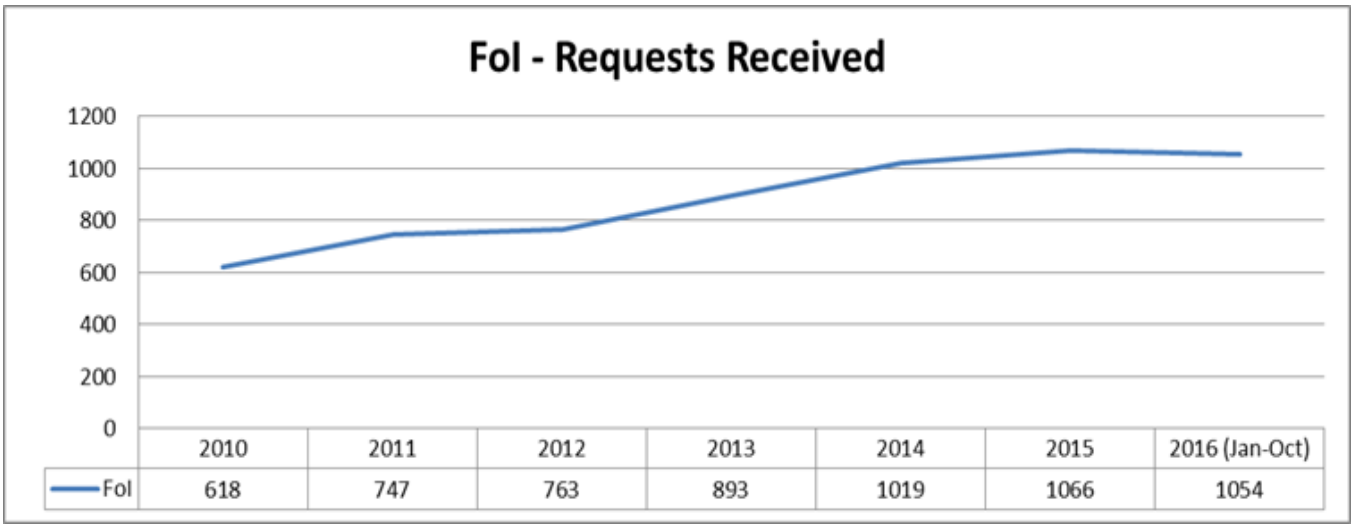
personal information relating to themselves this will be covered by the provisions of the Data Protection legislation whereas if a request is made for information which is not related to themselves this will be covered by the Freedom of Information Act 2000 (if the data is held by a public body).

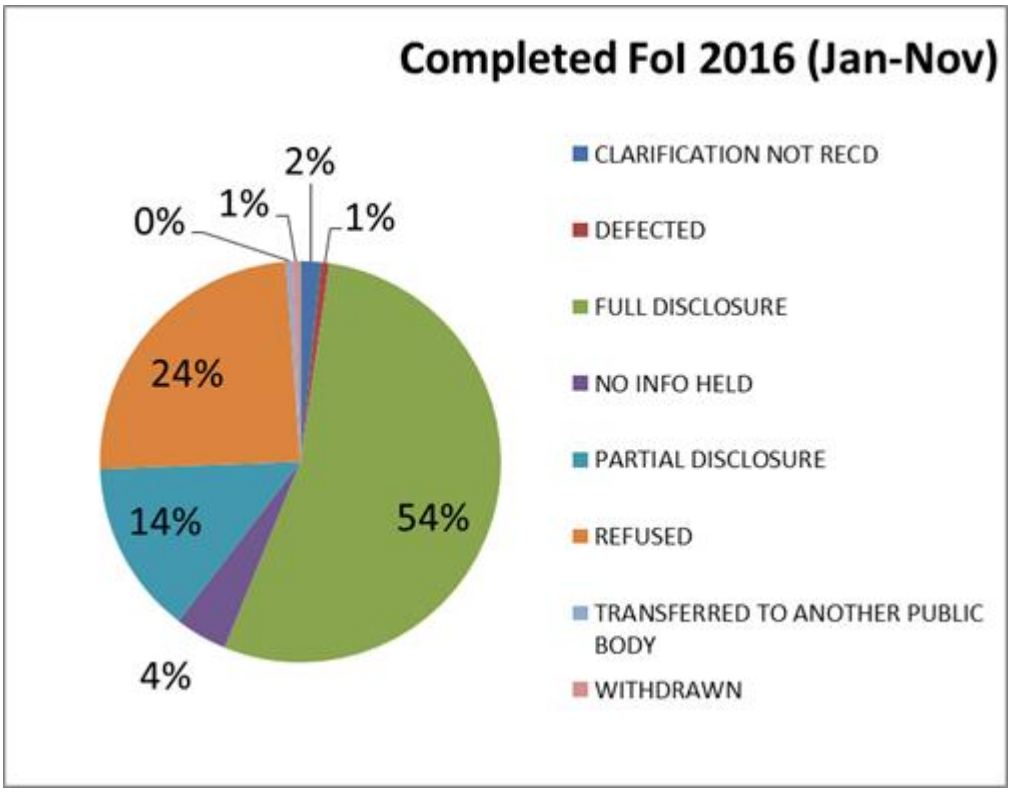
The Freedom of Information Act also requires public sector bodies to pro-actively publish certain classes of information within its publication scheme.

The trend in relation to requests under this piece of legislation continues to be one of growth. During the first year of the Act, the Constabulary received 252 requests. In 2015 the Constabulary received its highest volume of requests, since the legislation was enacted. Yet the year-end figures for 2016 are likely to show a further increase in demand of around 20%.

Following resource issues the Force has struggled in 2015 to meet the ICO minimum expectations in relation to compliance with statutory timescales (85%). During 2016 compliance rates have remained above 85%; however; if the trend growth continues through 2017 further challenges may emerge, when coupled with new demands from the changes to the data protection legislation.

Year	**2014**	**2015**	**2016 (up to 30 Sept)**
Requests received	1019	1066	932
Internal Reviews	10	18	20





Of the 20 internal reviews have been received to date, two cases have been subject to a decision notice by the Information Commissioner each of which found that the Constabulary had complied with its obligations.

The Constabulary continues to seek to publish information via its publication scheme; due to staff vacancies arising during the year some further work will be required to update the Scheme once the vacancies have been filled in 2017.

FOI – Independent Commission

In March 2016, the Independent Commission on FOI published its report which concluded that FOIA was generally working well and enhanced openness and transparency within the public sector. Some recommendations were made which if implemented would in due course likely have a resource implication.

MANAGEMENT OF POLICE INFORMATION (MoPI)

In 2015 HMIC published its report 'Building the Picture – An Inspection of Information Management'[1]. This report highlighted that Forces across the Country had departed from the national guidance on compliance with Statutory Code of Practice, and associated guidance, in relation to the Management of Police Information (MoPI).

Following the Report, a national police service project, which runs until December 2017, was established to consider the HMIC recommendations and to consider the present MoPI guidance. In Lancashire, the issues in relation to records management and MoPI were acknowledged and recorded on the Corporate Risk Register. A further Internal Audit Report was commissioned to review Information Management and Scrutiny.

[1] https://www.justiceinspectorates.gov.uk/hmic/publications/building-picture-an-inspection-of-police-information-management/

During the course of the year work has been on-going and continues in order to address the issues highlighted within both Reports. In particular :

Force Information Asset Owners have been identified and records updated. A training package for Information Asset Owners will be rolled out during 2017.

Work has been undertaken to review record retention practices across the Force.

From 2017 a new data protection breach/ security incident reporting process will be introduced. It will further assist in highlighting and identifying issues that should be recorded on the Force Information Risk Register.

All the work being undertaken in relation to the above will assist in helping achieve compliance with the requirements of the new Data Protection Regulatory framework.

A Force Records Manager has also been appointed. This is in recognition of the importance of good information management and its impact on operational policing. This dedicated resource will help to ensure a co-ordinated and informed approach to record keeping is maintained across the Force. They will also help inform the on-going ICT strategy, which will see various key force systems replaced in the short and medium term; some of the technological solutions procured will when fully implemented enhance information management and help facilitate MoPI compliance in the future. Whilst ICT solutions will assist in compliance with MoPI and the new data protection legislation, it is recognised that further consideration may be required of the appropriate human resource required within the functions of Information Audit and RRD (Review, Retention and Disposal) to ensure that data quality and record review and retention issues are addressed.

INFORMATION SECURITY

Within 2015-16, improvement has continued within the area of Information Security and has increased with the continued co-operation of ICT.

An external audit carried out of Information Security provided a greater impetus to improve and to meet its obligations.

During 2015, Lancashire Constabulary was one of the first police forces to achieve its Public Service Network in Policing (PSN(P)) accreditation and with it an improved security posture though continued technical improvements and due diligence.

In 2015 the Constabulary was also the first force to achieve national accreditation for its design to support the Child Abuse Image Database (CAID) system.

Cyber security is an increasing threat to the organisation and its data; as new risks and threats are introduced with continuing business demands and an ever evolving technological landscape. Investments in terms of technical controls continue and users are provided information and training to reduce the risks from within.

A formal system accreditation process has been introduced which provides a means of ensuring that risks introduced with new systems can be identified and mitigated against prior to any introduction.

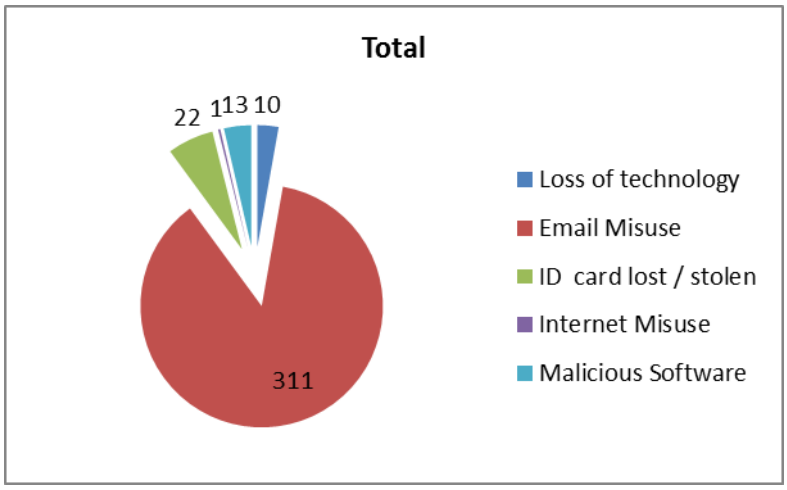
The greatest challenge for the Constabulary continues to be the demands, and with them risks to adopt evolving technology and for new services without compromising the safety of the organisation, its data, or its staff

Security Incidents[2]

As with all large organisations security incidents occur and are managed with rigour.

During the year 2015 the Constabulary suffered a number of incidents which are broken down into quarters in the table below.

Incident Type	Total
Loss of technology	10
Email Misuse	311
ID card lost / stolen	22
Internet Misuse	1
Malicious Software	13



The Constabulary continues to improve its security incident responsiveness. In 2015 the Constabulary was the victim of a cyber-attack involving thousands of spoofed emails. The response from the staff was exemplary, and as a result there was limited disruption to services and no loss of data or systems.

Any incident or security breach is analysed and processes and policies continue to evolve so as to reduce any future exposure and repetition.

Risks

Risks continue; with the greatest being its staff, especially with the increase of technology, applications, social media platforms, and the blurring of lines and perception.

Information Security should always be seen as an enabler, but also a critical friend. However conflict can occur with users; as in the drive to adopt new technology and social trends, many often ignore or overlook the risks that they may pose to the organisation, the consequences being financial and/or reputational damage.

Following a number of data breaches and attacks on UK police forces it is apparent that in common with other police forces and organisations, the greatest threat continues to be its staff.

[2] A security incident involves the actual loss, (or near miss), of personal or classified information assessed to present harm to an individual, a system, or the organisation

The Constabulary is improving and is beginning to develop the foundations of a security culture; but user error continues to be the highest threats to the organisation.

The explosion of data and the volume of information both internally and within the Internet, continues to increase with storage being available across a growing array of devices and media, all available to users within their personal lives.

The use of technology can considerably enhance business productivity because employees can now communicate from anywhere, at any time. However, this also creates a more complex environment with more potential areas of risk for the Constabulary.

With the fast changes within technology our information is now more exposed, being accessed from numerous devices, all with the ability to access Constabulary information. To combat this Constabulary has introduced a number of corporately owned devices, each serving a specific function**.**