REPORT TO: **JOINT MANAGEMENT BOARD**

DATE: **4 AUGUST 2017**

AGENDA ITEM: 3

SUBJECT: LANCASHIRE CONSTABULARY INFORMATION GOVERNANCE ANNUAL REPORT 2016/17

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 2016/17.

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.

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.

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 available 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	**2015**	**2016**	2017 (upto 30/6)
Requests received	260	288	185
ICO SA Complaints	4	8	6

The number of requests received in 2016 shows an increase of approximately 11% 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. As can also be seen from the half year figure, it would appear that there will be significant growth in the number of requests received during 2017. This growth is also reflected by the number of complaints received.

During 2016 the Constabulary responded to the Information Commissioner concerning eight complaints in relation to responses provided to subject access requests. It is expected that the trend in correspondence in relation to subject rights and complaints will increase with the additional subject rights that the new legislation will introduce from May, 2018.

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 December, 2017, the ICO decided to follow up a matter that had previously been the subject of complaint and assessment. A further review was undertaken by the ICOs Civil Investigations Team and it was concluded that regulatory action was not appropriate.

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 scope of what is to be considered for reporting is also extended. New procedures have been implemented by the Force to enable the new requirements to be met.

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 will be 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 2016, 96,000 checks were processed by the DBS team.

Demand in 2016 for the disclosure of police information for civil purposes and family court proceedings continues to grow. In 2016, 1111 family court disclosure applications were received and processed, an increase of 11% on the previous year.

INFORMATION SECURITY

One of the requirements of the Data Protection Act is to ensure that personal data is kept secure from unauthorised or unlawful processing and against accidental loss or destruction of, or damage to personal data. This is a specialised are within its own right and the Force seeks to comply with NPCC Community Security Policy. Within 2016-17, improvements have continued within the area of Information Security, this has been greatly assisted with the continued co-operation of ICT.

During 2017 Lancashire Constabulary has retained its Public Service Network in Policing (PSN(P)) accreditation and has seen a continued improvement in its security posture.

Over the past 12-months the Constabulary has introduced a number of changes including a formal system accreditation process, the new government security classifications, and technical controls and applications that will provide a more secure environment.

Cyber security continues to be an increasing threat to both the organisation and its data; as new risks and threats are introduced with continuing business demands and an ever evolving technological risk landscape.

In May 2017 the Wannacry ransomware attack targeted computers running the Microsoft Windows operating system by encrypting data and demanding payment. Within 24 hours this ransomware had infected more than 2 million computers in over 150 countries, including some parts of NHS causing it to run some services on emergency only basis. Lancashire was not affected by this malware due to the technical controls it deploys but will not remain complacent in its approach.

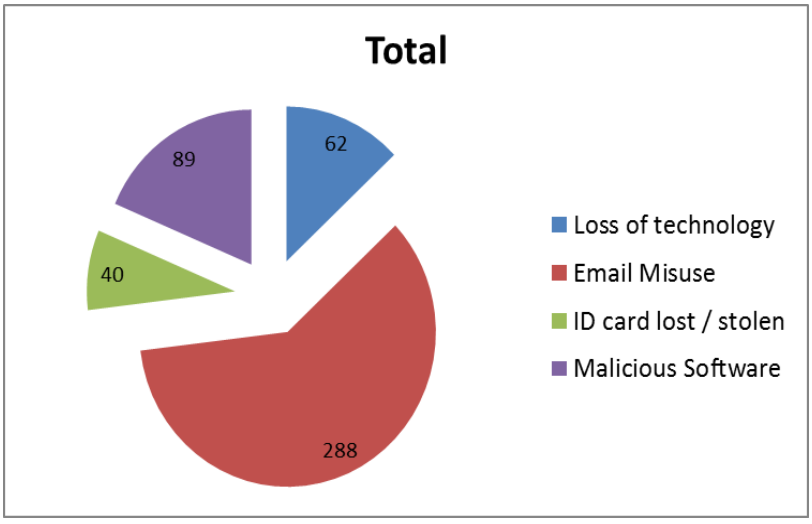
The greatest challenge for Information Security continues to be the technological demands, and with them risks in adopting new and evolving technology and services without compromising the safety of the organisation, its data, or its staff.

Due to the ever increasing technological advances, organisations need to be adequately prepared to deal with a cyber attack to ensure business continuity. In light of the recent threats the Constabulary is reviewing its Incident Response programme working for the first time with a commercial partner. This will enable the Constabulary to safeguard against the occurrence of such an attack, and enable it to respond more effectively should in the event of such an attack **Security Incidents[1].**

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

During the year 2016 the Constabulary suffered a number of incidents which are broken down in the table below.

Incident Type	Total
Loss of technology	62
Email Misuse	288
ID card lost / stolen	40
Malicious Software	89



[1] 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 continues to improve its security incident responsiveness, 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, especially with the increase of technology, applications, social media platforms, and the blurring of lines and the perception of risk. 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.

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, often ignore or overlook the risks that they may pose to the organisation with the consequences being financial and/or reputational damage.

The Constabulary is improving and is beginning to develop the foundations of a security culture, providing additional training and support; but user error continues to be the highest threat to the organisation.

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 continues to develop its methods of communication and increased technology that allows for safe, connectivity for officers and staff alike.

FREEDOM OF INFORMATION ACT 2000

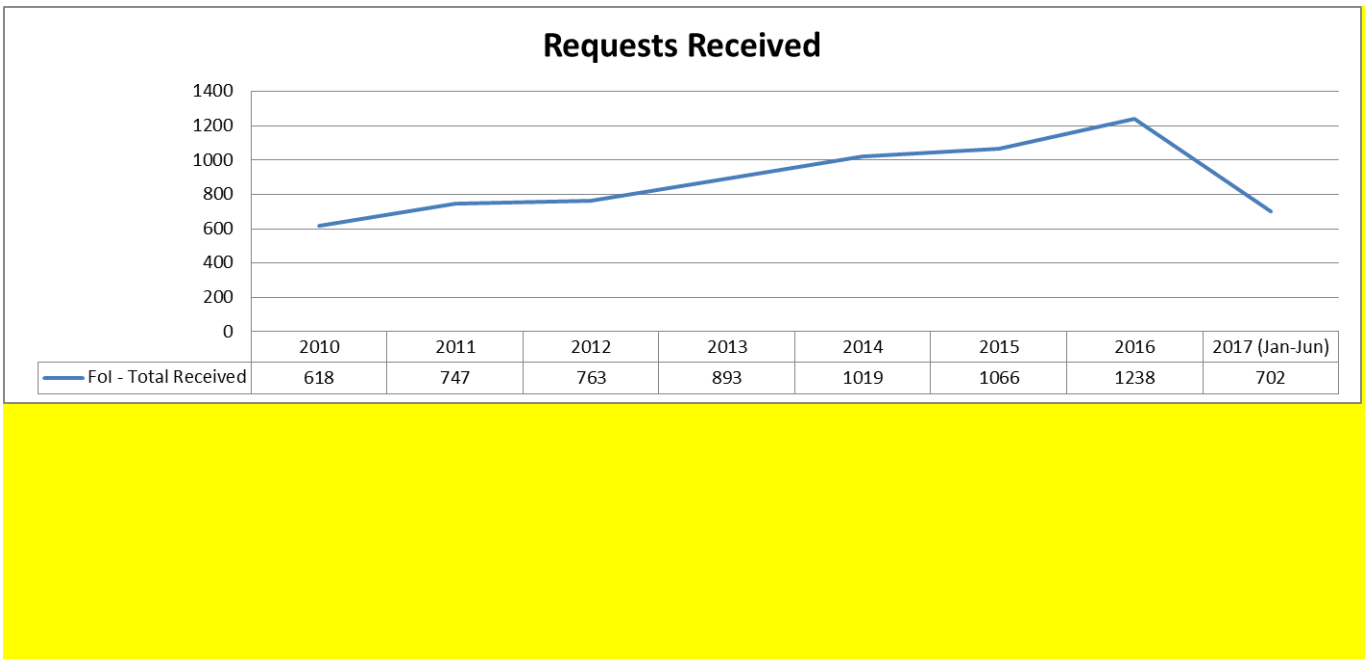
The Freedom of Information Act 2000 provides a right of access to information held by public bodies and is intended to be mutually exclusive to the Data Protection Act. So, if an individual requests access to personal information relating to themselves this will be covered by the provisions of the Data 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).

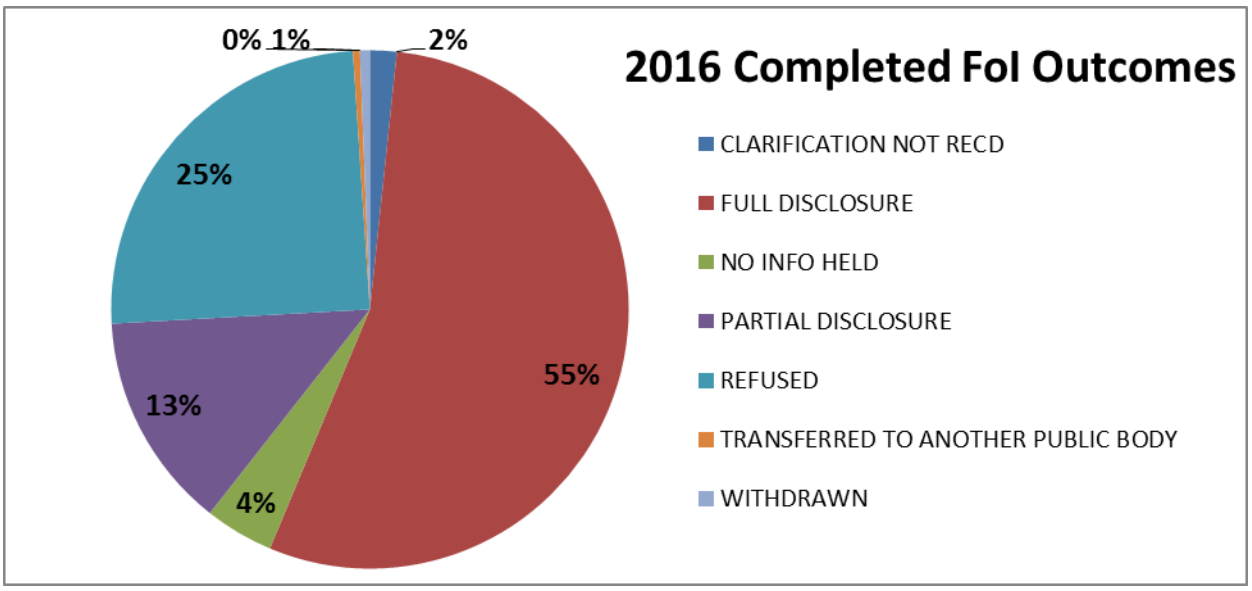
The Freedom of Information Act also requires public sector bodies to pro-actively publish certain classes of information within its publication scheme.

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 2016 the Constabulary received its highest volume of requests, since the legislation was enacted, with a 16% increase on 2015.

During 2016 compliance rates were 89%; however; the trend in growth has continued in 2017 to date and this may present further challenges. In particular, as the Information Commissioner has made it clear that public authorities should be compliant with statutory timescales in at least 90% of cases. As can be seen the numbers of complaints/ challenges (internal reviews) concerning the initial response has also increased.

Year	2015	2016	2017 (upto 30/6)
Requests received	1066	1238	702
Internal Reviews	18	20	17





Of the 20 internal reviews have were received in 2016, 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. Two cases have been subject to appeal to the Information Tribunal and have yet to be heard.

No ICO complaints have been received during the first six months of 2017.

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.

INTERNAL AUDIT REPORTS

In 2016/17 two Internal Audits have been conducted in relation to Information Management. The first sought to assess the adequacy and effectiveness of the Constabulary's arrangements in place to manage the receipt, processing and disclosure of information resulting from Freedom Of Information requests and Subject Access Requests in accordance with statutory requirements. The Audit Opinion was that substantial assurance was received regarding the adequacy and effectiveness of the Constabulary's arrangements for processing FOI requests and SARs. Some minor suggestions within a low risk area were made. It was noted that whilst many good practices were in place to process these requests, recent and forthcoming external changes to performance targets and data protection regulations will need to be considered and monitored by the Constabulary to ensure response effectiveness is maintained.

The second audit concerned the Information Management and Security framework. The main emphasis of the audit was to review the progress made by the Constabulary in implementing the actions agreed in the 2015/16 report issued in March 2016, focussing on the current framework of information security policies, related procedures and guidance.

The audit again found substantial assurance over the adequacy of the Constabulary's information management and security framework. The scope of the audit was such that it did not provide an opinion on the effectiveness of the framework. It was noted that actions had been taken since the last audit to improve the arrangements in place, in particular the steps taken toward compliance with MoPI (Management of Police Information) and APP (Authorised Professional Practice). Again, good practice was identified together with a suggested improvement within a low risk area. Whilst significant progress has been made, a number of the actions instigated to ensure full compliance were still on-going

The General Data Protection Regulation/ Law Enforcement Directive/ MOPI

The EU General Data Protection Regulation and Law Enforcement Directive will be transcribed in to a new Data Protection Act, which will take effect on the 6th May, 2018.

There will be significant implications for organisations and there are a number of implications for the Force in terms of its obligations arising from this new legislation. The new legislation seeks to achieve greater consistency across the EU & reflects change in the technological landscape over the past 20 years.

The main aspects of the new legislation are :

Greater obligations to demonstrate compliance (accountability)

Enhanced and increased rights for subjects

DP by design/ impact assessments

Much stronger penalties (20m euros)

Mandatory breach reporting

Mandatory “independent” data protection officer for public bodies and large processors with minimum tasks stated

Enhanced Records Management / data quality obligations.

New obligations for data processors (contractors / third parties with whom the data controller may engage)

Some aspects of the new legislation have yet to be finalised but the draft Bill should be published by September. The Force has commenced preparation for the new legislation and a programme of work established. The Force is represented on the NPCC Data Protection Reform Group and is also engaged with colleagues within the region. For police forces, compliance with the data protection legislation will be more complex. That is because there will be effectively two pieces of legislation that will need to be considered. Whilst there is much commonality, there are different requirements depending on whether the personal data is processed for crime/ non-crime purposes.

An important aspect of the new legislation is the ‘accountability’ principle and organisations will need to demonstrate that they have the appropriate governance, procedures, and resources in place to enable compliance. A key aspect in preparing for compliance is the work concerning records management and ensuring that information assets are documented and all data flows identified. This will also enable the Force to identify where data protection impact assessments might be required, which will consider the new requirements relating to fair processing/ consent/ lawful conditions. Progress in relation to this area of work will be assisted by two ‘Management of Police Information’ Audit posts that have recently been established. Engagement with Information Asset Owners during the autumn will help identify where compliance/ gaps may occur so that these can be addressed or recorded on an Information Management risk register.

New projects/ systems which involve the processing of personal data will need to consider the forthcoming changes and the additional compliance requirements. Training and awareness are factors included within the Force Action Plan.

The additional requirements in relation to ‘accountability’ and the enhanced rights for individuals are such that in 2017/18 there will be an increase in the demands for data protection officers and their compliance teams. This will require on-going assessment/ monitoring in terms of the resource requirement to meet the new statutory requirements.

Whilst we move towards the new compliance requirements from a statutory perspective, information management has also been subject to review from an operational perspective. In 2015 HMIC published its report ‘Building the Picture – An Inspection of Information Management’[2]. 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. A new Service Information Management Strategy will be published in 2017. This

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

will seek to bring about strategic direction and consistency across the service, taking account of business processes/ ICT so as to enhance data quality and accountability as we move towards a National Law Enforcement database.

During 2016/ 2017 the Force appointed a Force Records Manager. This is in recognition of the importance of good information management and its impact on operational policing. This dedicated resource is helping 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 will 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 human resources are also necessary. To this end, further investment has been undertaken in relation to the functions of Information Audit, RRD (Review, Retention and Disposal) and ensuring data quality. This will need to be kept under review as the national IM strategy is implemented.