London Ambulance Service NHS Trust

Data Protection Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To provide a framework to manage Data Protection legislation requirements

.

Sponsor Department: Information Governance

Author/Reviewer: Information Governance Manager. To be reviewed by May 2019

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
25/05/18	4.1	IG Manager	Document Profile and Control update
11/05/18	3.9	IG Manager	Major additions and other changes
20/11/17	3.8	IG Manager	Review. Minor amendment. Major review to be completed prior to new DP legislation May 2018
14/10/2016	3.7	IG Manager	Minor amendments
23/09/2015	3.6	IG Manager	Minor amendments
03/09/2014	3.5	IG Manager	Further minor updates following IGG 25/07/14
21/07/2014	3.4	IG Manager	Minor updates and changes to text
11/03/2013	3.3	IG Manager	Minor change to S.13 to reflect timescales in TP004 and PED address.
21/01/2013	3.2	IG Manager	Minor change to S.12 identifying specific arrangements for SARs agreed by IGG.
27/09/2011	3.1	IG Manager	Minor changes required by ADG: S.5 added & 1st bullet point in S.7 changed.
23/02/2011	2.3	Head RM	Further Revision
14/01/2011	2.2	Head RM	Revision
06/07/2010	2.1	Records Manager	Reformat
March 2007	2.0	Director IM&T	
March 2003	1.0	Director IM&T	

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
PMAG	18/05/18	4.0
IGG	20/10/16	3.7
IGG	30/09/15	3.6
ADG	24/08/11	3.0
	03/07	2.0
Chief Executive	03/03	1.0
Ratified by (If appropriate):		
ELT	25/05/18	4.0

Published on:	Date	By	Dept
Thw Pulse	25/05/18 (v4.1)	Internal Comms team	Comms
The Pulse	01/02/18 (v3.8)	Digital Media Officer	Comms
The Pulse	31/10/16 (v3.7)	Governance Administrator	G&A
The Pulse	17/11/15 (v3.6)	Governance Administrator	G&A
The Pulse	11/09/14 (v3.5)	Governance Administrator	G&A
The Pulse	28/12/11	Governance Co-ordinator	GCT
LAS Website	25/05/18 (v4.1)	Internal Comms team	Comms
LAS Website	01/02/18 (v3.8)	Digital Media Officer	Comms
LAS Website	31/10/16 (v3.7)	Governance Administrator	G&A
LAS Website	17/11/15 (v3.6)	Governance Administrator	G&A
LAS Website	11/09/14 (v3.5)	Governance Administrator	G&A
LAS Website	28/12/11	Governance Co-ordinator	GCT
Announced on:	**Date**	By	Dept
The RIB	04/06/18	IG Manager	IG
The RIB	01/11/16	IG Manager	G&A

EqIA completed on	By
21/03/11	C D-B; SM; BO
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
TP/048	LAS Information Security Policy	
TP/004	Complaints Procedure.	
TP/057	Waste Management Policy	
TP/022	Freedom of Information Policy	
TP/009	Policy for Access to Health Records, Disclosure of Patient Information, Protection and Use of Patient Information	
TP/017	LAS Procedure for Health Records	
TP/024	Managing Patient Confidentiality when Dealing with the Media	
TP/029	Records Management & Information Lifecycle Policy	
TP080	Social Media Policy	
	Information Commissioners Office guidance on Data Protection.- www.ic.gov.uk/guidance	
	Data Protection Act 2018	
	Regulations of Investigatory Powers Act, 2000	
	The Information Governance Review (Caldicott 2) 2013 and Caldicott 3)	
	Computer Misuse Act, 1990	
	Access to Health Records Act, 1990	
	Directive on Privacy and Electronic Communications, 2002	
	The Privacy and Electronic Communications Regulations, 2003	
	Human Rights Act, 1998	

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Introduction

This policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards under the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR).

The new DPA seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data. It supplements the GDPR as well as extends data protection laws to areas which are not covered by the GDPR. The DPA also ensures a single regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector.

The DPA and GDPR legislates for the protection of personal information relating to living individuals. The Access to Health Records Act 1990 will remain relevant for information relating to deceased persons.

The nature of the work undertaken by the Trust's employees, volunteers and contractors brings them into possession of a great deal of confidential, and often highly sensitive information, both patient and staff related. Therefore, it is essential that the public at large have confidence that the organisation as a whole maintains confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose.

2. Scope

This policy covers all sites and systems operating and utilised by the LAS. It is applicable to all staff, volunteers, companies and other third parties holding, storing or using information for or on behalf of the LAS

3. Objectives

1. To provide a framework to manage Data Protection legislation requirements.

2. To provide guidance to staff and third parties that explains the requirements of the legislation and their responsibilities with regard to managing an individual's personal information.

4. Responsibilities

4.1 The **Trust Board** is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives. The Trust as a body corporate is a data controller.

4.2 The **Chief Executive** has overall responsibility for ensuring that compliance with Data Protection legislation is managed responsibly within the Trust.

4.3 The **Director of Corporate Governance** has strategic responsibility for Information Governance including compliance with the Data Protection Act throughout the Trust.

4.4 The **Caldicott Guardian** is responsible for protecting the confidentiality of patient and service-user information and this policy supports the Caldicott function.

4.5 The **Chief Information Officer** is the Senior Information Risk Owner (SIRO) and has strategic responsibility for the management for information risk.

4.6 The **Data Protection Officer** is responsible for providing specialist data protection advice and for developing specific guidance notes on data protection issues. The DPO is responsible for ensuring payment of administrative fees in respect of the legislation to the Information Commissioners Office (ICO). The DPO also has the responsibilities laid out in Article 39 of the GDPR – see Appendix 1.

4.7 The **Information Governance Manager** is responsible for providing day-to day advice on data protection matters.

4.8 The **Information Security Management team** is responsible for information security in the LAS and provides relevant support for data protection related issues.

4.9 The **Head of Patient Experiences** is responsible for the handling and processing of Subject Access Requests by the Patient Experiences Department made under the legislation.

4.10 The **Head of Workforce Analytics** is responsible for coordinating the handling of Subject Access Requests received from staff and ex-staff.

4.11 The **Information Governance Group (IGG)**, chaired by the Chief Information Officer who is the Senior Information Risk Owner (SIRO) and the Director of Corporate Governance, will monitor the implementation of this policy.

4.12 The **Executive and Senior Management Teams** and **Heads of departments** are responsible for ensuring that the policy is implemented in their directorates and individual departments.

4.13 All staff are responsible for ensuring that the principles outlined within this policy are universally applied. Compliance with Data Protection legislation is the responsibility of all members of the Trust who process personal information and this includes contractors, temporary staff and students.

5. Definitions

5.1 **Data Controller**
The legal person, or organisation, which determines the purpose and means of the processing of personal data.

5.2 **Data Processor**
The legal person, or organisation, which processes personal data on behalf of the controller.

5.3 **Data Subject**
The identified or identifiable living individual to whom personal data relates.

5.4 **Identifiable living individual**
Living individual who can be identified, directly or indirectly, in particular by reference to:

- an identifier such as a name, an identification number, location data or an online identifier; or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

5.5 **Information Commissioner**
Independent body set up to uphold information rights.

5.6 **Personal data**
Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5.7 **Processing**
In relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

- collection, recording, organisation, structuring or storage;
- adaptation or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; or
- restriction, erasure or destruction.

6. Enforcement

Any employee deliberately acting outside of their authority will be subject to LAS disciplinary procedures, up to and including dismissal where appropriate, and to possible legal action by the LAS. Any action to initiate legal proceedings shall be approved by either the Chief Executive, or the Director of Corporate Governance.

7. Data Protection Legislation

The 2018 Data Protection Act (DPA) assists with and supplements the adoption of the GDPR into UK law. It strengthens or provides exceptions from some of the requirements of the GDPR and also extends data protection law into types of processing that are not covered by the GDPR. The DPA provides the Information Commissioner with additional functions and introduces new powers and offences in relation to data protection. The DPA applies to staff as well as patient records and covers both paper and electronic records.
Any individual has the right to see what information is held about them and may challenge this information if they feel it is inaccurate or has caused damage to them. The DPA places obligations on those who record and use information about individuals. They must register the use of that information and they must ensure that they follow sound practices in recording and using the information.

7.1 Data Protection Principles

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

7.2 Lawful basis for processing

There must be a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

The lawful basis must be determined and documented before processing. The LAS privacy notice will include the lawful basis for processing as well as the purposes of the processing. Processing of special category data requires both a lawful basis for general processing and an additional condition for processing.
The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:
(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract with the individual, or because the individual has asked the LAS to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for the LAS to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for the LAS to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply to public authorities processing data to perform official tasks.)

7.3 Special category data

When processing special category data it is necessary for the LAS to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. We will document both our lawful basis for processing and our special category condition so that we can demonstrate compliance and accountability.

Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. The choice of lawful basis under Article 6 does not dictate which special category condition must be applied, and vice versa. For example, if consent is used as the lawful basis, there is no restriction to using explicit consent for special category processing under Article 9. The most appropriate special category condition in the circumstances should be chosen

– although in many cases there may well be an obvious link between the two. For example, if the lawful basis used is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of their personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health

care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7.4 Individual Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The lawful basis for processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	×
Contract	✓	✓	×
Legal obligation	×	×	×
Vital interests	✓	×	×
Public task	×	×	✓
Legitimate interests	✓	×	✓

However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies. The remaining rights are not always absolute, and there are other rights which may be affected in other ways.

7.5 Data Subject Rights

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Further information is provided in the Subject Access Procedure.

7.6 Personal Data Breaches

The LAS is required to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individual must also be informed without undue delay. The LAS will maintain records of any personal data breaches in the Datix system regardless of whether we are required to notify.

7.7 Accountability and Governance

Under the legislation the LAS is responsible for complying with the GDPR and must be able to demonstrate compliance. We will:

- Put in place appropriate technical and organisational measures to meet the requirements of accountability.
- Adopt and implement data protection policy and procedural documents.
- Take a 'data protection by design and default' approach.
- Put written contracts in place with organisations that process personal data on our behalf.
- Maintain documentation of processing activities.
- Record and, where necessary, report personal data breaches.
- Carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.
- Appoint a data protection officer.

The obligations that accountability places on the LAS are ongoing. It is not simply signing off a particular processing operation as 'accountable' and moving on. Measures implemented must be reviewed at appropriate intervals to ensure that they remain effective and updated when required.
The LAS must be able to show that it has considered the risks to personal data and put in place measures and safeguards to provide mitigation against any potential data breaches.

8. Statement of Intent

The LAS intends to fulfil all its obligations under the new legislation including ensuring that its registration details with the ICO are accurate and up to date. The LAS will secure and maintain in accordance with the legislation such data as is necessary to assist in the protection of the health and safety of its staff while continuing to comply with obligations to patients and others under the legislation. Where the LAS is not the data controller but rather the data processor it will abide by any written agreement between it and the data controller on data protection policy.

9. Privacy by Design

As required by the legislation all new projects and initiatives will be checked to ensure that wherever personal data is involved a Data

Privacy Impact Assessment is carried out to document the measure put in place to protect personal data. This is documented in TP059 Data Privacy Impact Assessment Policy and Procedure.

10. Privacy Notices

The LAS will, as far as is practicable, ensure that all individuals whose details it holds are aware of the way in which that information will be held, used and disclosed. Individuals whose information is held and processed by the LAS can be assured that it will treat their personal data with all due care and Privacy Notices will be provided to show the LAS use of personal data and the legal basis for processing. If a person feels they have been deceived or misled as to the reason for which their information was collected, they should use the complaint process detailed at the end of this document. There is a Privacy Notice on the LAS website which states 'How we use your personal information'.

11. Information Sharing

The LAS will share personal information with other agencies where it is legal to so do if this enhances its ability to provide services that affect a person's health or where the LAS needs the support of another agency to ensure the best patient care for an individual. Where required information sharing arrangements concerning Patient Confidential Data (PCD) will be based upon formal protocols and information sharing agreements which will document the legal basis for sharing. An Information Sharing Policy is being developed to provide further detail on our approach to information sharing.

12. Training

It is the aim of the LAS that all appropriate staff are properly trained, fully informed of their Data Protection obligations and are aware of their personal responsibilities. All staff will receive mandatory data security training on an annual basis and specialist Data Protection training will be provide to staff who handle sensitive personal data on a regular basis. The LAS Confidentiality Code of Conduct outlines the obligations of all staff to ensure that access to personal data is appropriate, kept secure and not disclosed inappropriately.

13. Data Quality and Integrity

The LAS will not collect data from individuals where that information is excessive or irrelevant in relation to the purpose(s). Details collected will be adequate for the purpose and no more. Information collected which becomes (over time or by virtue of changed purposes) irrelevant or excessive will be deleted. All of the LAS directorates/departments will manage data collection and updating of records such that accuracy, relevance consistency with purpose and quality are assured.

Information will only be retained for as long as is necessary after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will always be done within the requirements of the legislation. In some cases personal details will be removed from the record or pseudonymisation will be used so that individuals cannot be identified.

The LAS will ensure, as far as is practicable, that the information held is accurate and up to date. It is the intention of the LAS to check wherever possible the details given. Information received from third parties (i.e. neither the individual concerned nor the LAS) will indicate the source, where practicable.

Where a person informs the LAS of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a comment will be placed on the disputed record indicating the nature of the problem. If the system does not allow the individual record to be marked in this way, departments will ensure that a manual record is made of the request and that it is processed within a reasonable time-scale.

Every effort will be made to reach an amicable agreement on any disputed data. Where this is not possible the LAS will implement its complaints procedure.

An internal investigation will be implemented if there is any alleged improper misuse of personal data by staff and appropriate action will be taken.

If a staff member suspects any weaknesses in the security of any information processing systems or suspects staff misuse with regard to data protection they should contact the Data Protection Officer.

14. Technical and Organisational Security

The LAS has implemented appropriate security measures as required under the legislation. These are set out in full in the LAS's Information Security Policy. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place and all LAS buildings have reception areas or controlled access.

Computer systems are installed with user-profile type password controls to ensure data is only accessed by authorised users, and where necessary, audit and access trails are monitored to establish that each user is fully authorised. In addition, all portable media is

protected by encryption. Manual filing systems are held in secure locations and are accessed on a need-to-know basis only.

The Information Governance Group regularly review Security arrangements and reported breaches of security are investigated. Where necessary, further or alternative measures are introduced.

Where details need to be passed outside the LAS it will be done a required by the legislation. Any unauthorised disclosure will be dealt with under the LAS's disciplinary procedures.

Redundant personal data will be destroyed as confidential waste in line with TP057 Waste Management Policy. In general, paper waste is shredded internally by cross-cut shredders or by outside certified contractors under local agreements and magnetic media (disks, tapes, etc.) are either electronically wiped or physically destroyed beyond recovery.

15. Subject Access/Subject Information Requests

The legislation gives individuals the right to see information held about them and it places a duty on the LAS to make that information available. Thus any person whose personal details are held/processed by the LAS has a right to receive a copy of his or her own information without payment of a fee. There are a few exceptions to this rule (examples being data held for child protection, crime detection/prevention purposes or where the information is likely to cause serious harm to the physical and/or mental health of the patient or other individual) but most individuals will be able to have a copy of the data held about them.

Where any information relates to an identifiable third party, other than the data subject, consent must be gained from that third party, before any information relating to them can be released.

Any codes used in the record will be fully explained; any inaccurate, out of date, irrelevant or excessive data will be dealt with under the procedures outlined in section 13 of this document, Data Quality and Integrity.

Subject access requests from the public or solicitors acting on behalf of the public will be handled by Patient Experiences Department; those from the police will be handled by Operational Information and Archives; those from staff and ex-staff will be handled by Human Resources. A subject access request process or procedure is being developed which will provide further detail.

The LAS will reply to subject access requests as quickly as possible and usually within the 30 days allowed by the legislation unless the request is of a complex nature. Repeat requests will be fulfilled unless the period between is deemed unreasonable, such as a second

request received so soon after the first that it would be unlikely for the details to have changed. The LAS will endeavour to fulfil all legitimate and reasonable requests. In some cases further information may be required from the requester which may delay the start of the 30 day maximum time limit.

16. Further Information, Enquiries and Complaints

The LAS Data Protection Officer is the first point of contact on any of the issues mentioned in this policy document. The Patient Experiences Department handles all external complaints. Where possible, requests for detailed information should be in writing.

Any complaints must be written, dated, and must include details of the complainant as well as a detailed account of the nature of the problem. The LAS will aim to provide a substantive response within twenty five working days and in every case the person will receive an acknowledgement within three working days of the complaint being received.

Complaints should be sent to the Patient Experiences Department who can be contacted by telephone on 020 3069 0240 or by writing to them at:

London Ambulance Service NHS Trust, Units 1 & 2, Datapoint Business Centre, 6 South Crescent, London E16 4TL.

or email: ped@londonambulance.nhs.uk

IMPLEMENTATION PLAN	
Intended Audience	All LAS Staff
Dissemination	Available to all staff on the Pulse and to the public on the LAS website.
Communications	Revised Policy to be announced in the RIB and a link provided to the document.
Training	DP training is provided to new staff at Corporate Induction and to existing staff by annual online IG training. See also S.12 of this policy.

Monitoring:

Aspect to be monitored	**Frequency of monitoring AND Tool used**	**Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported**	**Committee/ group responsible for monitoring outcomes/ recommendations**	**How learning will take place**
Compliance with the Act through review of incidents	Quarterly	DP Officer Information Governance Group	RCAG	Revision of policy and training.

Appendix 1

Article 39 – Tasks of the DPO

(1) The data protection officer shall have at least the following tasks: a) to inform and

advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

d) to cooperate with the supervisory authority;

e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.