Data Protection and Security Policy

Data Protection and Security Policy		Page:	1 of 14
Author:	Data Protection Officer	Version:	2.0
Date of Approval:	11th July 2019	Status:	Final
Date of Issue:	7th August 2019	Date of Review	1st July 2021

Recommended by	Information Management Group
Approved by	Information Management Group
Approval date	11th July 2019
Version number	V2.0
Review date	1st July 2021
Responsible Director	Senior Information Risk Owner
Responsible Manager (Sponsor)	Information Governance Manager
For use by	All staff

This policy is available in alternative formats on request. Please contact the Corporate Governance Office on 01204 498400 with your request.

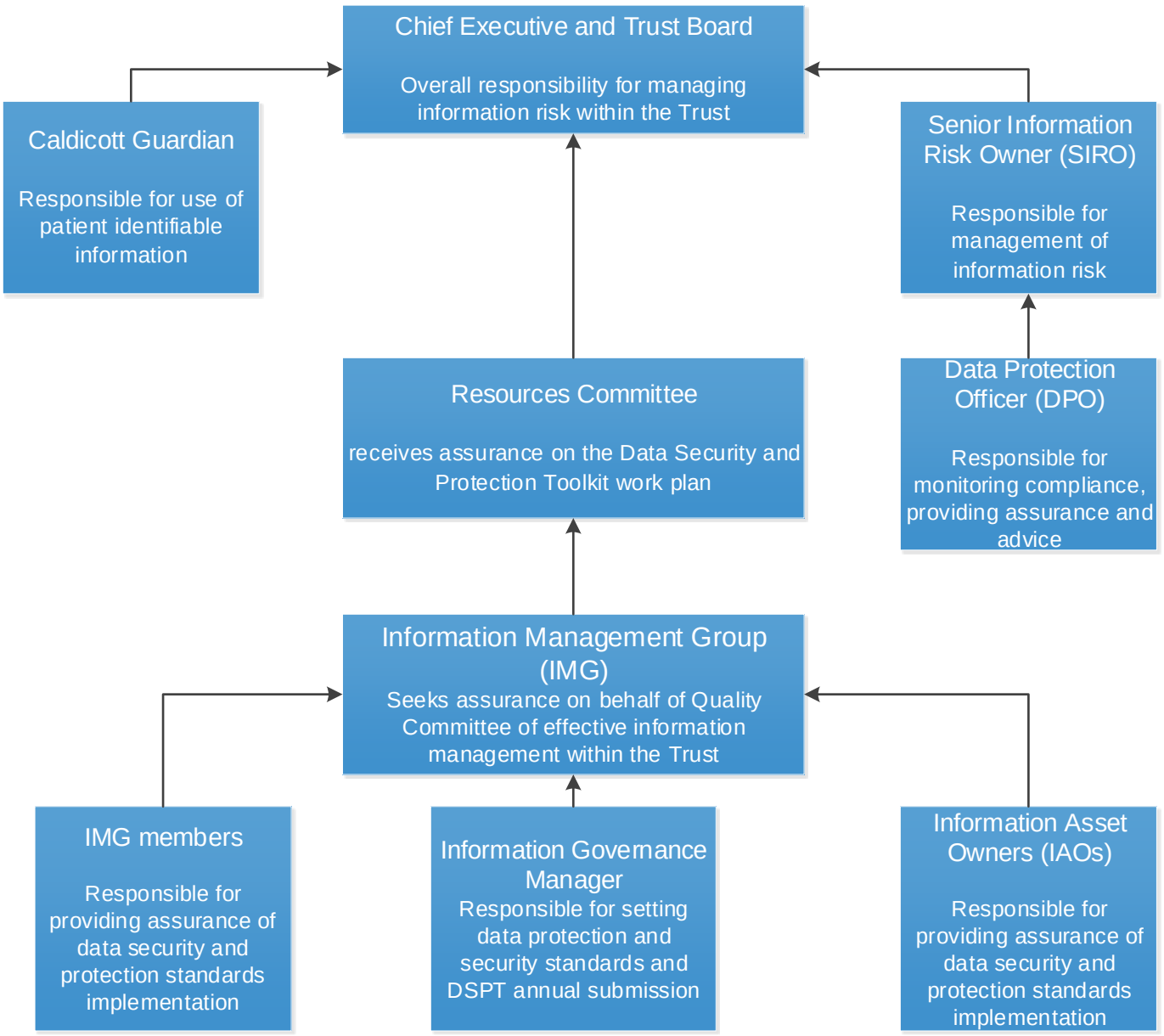
Change record form

Version	Date of change	Date of release	Changed by	Reason for change
0.1	03/07/2018	N/A	Robin Ellis	DPSP drafted to consolidate the following existing Trust documents: Information Governance Policy Information Governance Strategy Information Security Policy Information Sharing Policy Confidentiality Policy Data Quality Policy
1.0	03/07/2018	30/10/2018	Joanne Moran	Review of Draft V0.1. Approval of content for adoption by the Trust
2.0	18/03/2019	07/08/2019	Joanne Moran	Section 1 Data Security and Protection Structure - Quality Committee has been updated to Resources Committee Section 4 Duties - Quality Committee has been updated to Resources Committee Section 7.6 - links to the Privacy Notices have been added Section 8.4 – Information Security documentation explanation added Section 10.3 – A link to the Clinical Records Policy has been added Section 11.4 Education & Awareness - has been updated to reference the Trust Training Needs Analysis for Information Governance mandatory training. Section 14 – Lists of governing standards, guidance and procedures have been added with links to their location on the Trust intranet. Section 1 Data Security and Protection Structure Finance Improvement and Planning changed to Resources Committee

Data Protection and Security Policy

Contents

1. Data Security and Protection Structure



2. Introduction

2.1. Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service delivery and performance management.

2.2. Data protection is concerned with the way NHS organisations handle information about patients and employees, in particular personal and sensitive information. It enables organisations and individuals to deal with personal information legally, securely, efficiently and effectively in order to deliver the best possible care.

2.3. The North West Ambulance Service NHS Trust (NWAS or, "the Trust") is committed to meeting the information needs of patients, healthcare professionals and staff, policy makers and managers and the public.

2.4. It is the intention that this policy and associated documents will be reviewed and updated following any major changes to legislation and/or applicable policy or every 12 months, whichever is sooner.

3. Purpose

3.1. The purpose of this Data Protection & Security Policy is to provide guidance in line with sector best practice that is appropriate for the Trust to allow relevant departments to produce the necessary policy and guidance for their area and to ensure that the applicable and relevant data protection controls are in place in line with the Department of Health, the wider NHS and health and social care requirements.

3.2. Definitions

Term	Meaning/Application
Shall	This term is used to state a **Mandatory** requirement of this policy
Should	This term is used to state a **Recommended** requirement of this policy
May	This term is used to state an **Optional** requirement

4. Duties

4.1. The Trust's responsibilities regarding data protection are as follows:

4.1.1. The Trust Board: The Trust Board shall define the Trust policy in respect of information governance, taking into account legal and NHS requirements. The Board shall ensure that sufficient resources are provided to support the requirements of this policy. The Chief Executive and Trust Board are personally accountable for the records in their care and quality of records management within their organisation.

4.1.2. Resources Committee: The Resources Committee shall seek assurance on behalf of the Board of Directors of the completion of the Data Security & Protection Toolkit workplan. The committee is therefore accountable to the Board. The Director of Quality, Innovation and Improvement, who is also the Senior Information Risk Owner attends the Resources Committee meetings.

4.1.3. Information Management Group (IMG): The IMG shall be responsible for overseeing the implementation of the Data Security and Protection strategy, this policy, the Data Security and Protection Toolkit (DSPT) improvement and work plan and other relevant policies as set out in the IMG Terms of Reference (Appendix A). The IMG is accountable to the Resources Committee.

4.1.4. Senior Information Risk Owner (SIRO): The SIRO shall have ultimate responsibility for the management and mitigation of risks associated with the Trust's information management processes.

4.1.5. Caldicott Guardian: The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use and sharing of patient identifiable information.

4.1.6. Data Protection Officer (DPO): The DPO shall provide a central point of contact for enquiries from patients, staff and the supervisory authority (Information Commissioner's Office) regarding current data protection legislation. They shall monitor the Trust's compliance with data protection legislation and provide advice to the Trust on the same.

4.1.7. Information Governance Manager: The Information Governance Manager, supported by the Information Governance Team, shall be responsible for overseeing day-to-day Information Governance issues, including developing and maintaining policies, standards, procedures and guidance and raising awareness of Information Governance. The Information Governance Manager is responsible for providing the Trust with advice and guidance on information governance issues and best practice. The Information Governance Manager coordinates the assurance reports for IMG and the annual audit submission to the DSPT.

4.1.8. Information Asset Owners (IAOs): IAOs supported by the Information Governance Manager, shall be responsible for understanding and addressing the risks to the information assets they "own" as part of operational management. IAOs shall be accountable for the safe storage and usage of the information contained in "their" information assets.

4.1.9. All Managers: Managers within the Trust shall be responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance with them in their area. All line managers and supervisors also have a duty to ensure that their staff are adequately trained in information governance through completion of mandatory training.

4.1.10. All Staff: All staff, whether permanent, temporary or contracted shall be responsible for ensuring that they are aware of the requirements incumbent upon them ensuring that they comply with them on a day to day basis.

5. Data Protection Principles

5.1. NWAS recognises the need for an appropriate balance between data protection and transparency in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard both personal information about patients and staff and commercially sensitive information.

5.2. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the public interest. This is controlled by the Information Sharing procedure.

5.3. The Trust understands that accurate, timely and relevant information is essential to deliver the highest quality health care. As such, it shall be the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

5.4. There are four key strands to the data protection policy: transparency, legal compliance, information security and quality assurance.

6. Transparency

6.1. Non-confidential information about the Trust and its services shall be available to the public through a variety of media.

6.2. The Trust shall establish and maintain policies and procedures to ensure compliance with the Freedom of Information Act 2000 and current data protection legislation.

6.3. The Trust will undertake or commission annual assessments and audits of its information management policies and arrangements to promote transparency. Patients should have ready access

to information relating to their own healthcare, their options for treatment and their rights as patients. Staff should have ready access to information the Trust holds about them.

6.4. The Trust shall have clear procedures and arrangements for liaison with the press and broadcasting media.

6.5. The Trust shall have clear procedures and arrangements for handling queries from patients and the public.

6.6. The Trust shall share information with other health care providers, local authorities or external companies. Where this happens sharing shall comply with internal procedures and current data protection legislation.

7. Legal Compliance

7.1. The Data Protection Act (DPA) assists with and supplements the adoption of the General Data Protection Regulation (GDPR) into UK law. It strengthens or provides exceptions form 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.

7.2. The DPA places obligations on those who record and use information about individuals. They shall register the use of that information and they shall ensure that they follow sound practices in recording and using the information.

7.3. There shall be a valid lawful basis in order to process personal data. 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. Advice and guidance may be sought from the Data Protection Officer.

7.4. The lawful basis shall be determined and documented before processing. The Trust privacy notice should include the lawful basis for information processing as well as the purposes of the processing. Processing of special category data (previously known as sensitive data) requires both a lawful basis for general processing and an additional condition for processing.

7.5. The GDPR provides the following rights for individuals:

- **7.5.1.** The right to be informed
- **7.5.2.** The right of access
- **7.5.3.** The right to rectification
- **7.5.4.** The right to erasure
- **7.5.5.** The right to restrict processing
- **7.5.6.** The right to data portability
- **7.5.7.** The right to object
- **7.5.8.** Rights in relation to automated decision making and profiling.

7.6. The Trust obligations to inform patients and staff about the data processing it carries out are met by the Trust Privacy Notices which can be found:

7.7. https://www.nwas.nhs.uk/help/privacy/

- **7.7.1.** https://intranet.nwas.nhs.uk/have-your-say/staff-privacy-notice/

7.8. The lawful basis for processing can also affect which rights are available to individuals.

7.9. Accountability is one central tenents of current data protection legislation, it makes the Trust responsible for complying with the GDPR and says that we shall be able to demonstrate compliance.

7.10. The Trust will:

- **7.10.1.** Put in place appropriate technical and organisational measures to meet the requirements of accountability.
- **7.10.2.** Adopt and implement data protection policies.
- **7.10.3.** Take a 'data protection by design and default' approach.
- **7.10.4.** Put written contracts in place with organisations that process personal data on our behalf.
- **7.10.5.** Maintain documentation of processing activities.

7.10.6. Record and, where necessary, report personal data breaches.

7.10.7. Carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.

7.10.8. Appoint a Data Protection Officer.

7.11. The obligations that accountability places on the Trust are ongoing, it is not simply signing off a particular processing operation as 'accountable' and moving on. There shall be a review of the measures implemented at appropriate intervals to ensure that they remain effective and updated where no longer fit for purpose.

7.12. If something does go wrong, then being able to show that the Trust actively considered the risks and put in place measures and safeguards can help provide mitigation against any potential enforcement action. If good data protection practices cannot be shown, it may leave the Trust open to fines being levied by the Information Commissioner and reputational damage.

8. Information Security

8.1. The core information security principles that protect information assets and data are:

8.1.1. Confidentiality (C) – protecting information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.

8.1.2. Integrity (I) – retaining the integrity of the information/data by not allowing it to be modified.

8.1.3. Availability (A) – maintaining the availability of the information/data by protecting it from disruption and denial of service attacks.

8.2. In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A principles are breached.

8.3. Any data breach related to patient or staff data shall be categorised according to which element or elements of the information security principles apply to the breach, reported following the data breach reporting procedure and investigated according to the Trust investigations procedure and standards.

8.4. Information Security shall be governed by standards set out in Principal Standards, Guidelines and Procedures which are detailed in section 14 of this policy.

9. Quality Assurance

9.1. The Trust shall undertake or commission annual assessments and audits of its information quality and records management arrangements.

9.2. Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

9.3. Information quality should be assured at the point of collection. Departments/teams shall have local procedures that include measures to provide this assurance.

9.4. NWAS, like all healthcare providers in the NHS, is required to report information to Government Departments as part of operational governance. The Trust commits to providing the minimum data wherever possible, providing this does not impact the purpose of the reporting. The Trust may use the following to achieve this purpose:

9.4.1. Aggregation: Any process that counts the number of occurrences where records in a data set meet specific criteria. The end product is statistics that are derived from a data set therefore there is no way of knowing whose records made a contribution to those numbers.

9.4.2. Anonymisation: A process by which all identifiers relating to individual persons are removed from records, thereby rendering them anonymous by producing new records that cannot be traced back to the person whose data is contained in the record.

9.4.3. Pseudonymisation: A process that replaces all identifiers relating to an individual a person by a pseudonymised key which could (with some effort) be mapped back to the person whose data is contained in the record.

10. Records Management

10.1. Clinical records management is governed by the Clinical Records Policy and advice should be sought from the Clinical Records Manager as and when required.

10.2. Corporate records management is delegated to local department/team managers. NWAS as a Trust will adhere to the NHS Records Management Code of Practice 2016 and the retention schedules for records contained within it. Advice and guidance on local implementation of this Code of Practice shall be provided by the IG Manager.

10.3. The Trust has a Clinical Records Policy that details processes on protecting patient's information. It can be found here.

11. Education and Awareness

11.1. All staff (permanent, part-time, temporary, contractors and third parties subcontracted as information processors) of NWAS shall receive the NHS Digital provided Data Security Awareness Training (or an independently verified equivalent) at least annually. This may be delivered through a variety of media.

11.2. Additional relevant training shall be undertaken by the SIRO, Caldicott Guardian and DPO.

11.3. Departments/teams should actively seek guidance on the level of training they may need to undertake in the area of data protection as and when their responsibilities change. This advice should be sought from the DPO.

11.4. All staff shall complete mandatory training the Trust has agreed to use NHS Digital learning materials i.e Data Security and Awareness e learning. This has been approved by the Trust Board and is detailed in the Training and Needs Analysis (TNA) that is managed by the Learning & Development (L&D) team. Monitoring of the TNA is also a responsibility of the L&D team. Percentage of staff completing training is submitted to NHS Digital via the final submission of the Data Security & Protection Toolkit.

12. Monitoring Compliance

12.1. Compliance with this policy will be undertaken as summarised in the table below. Any identified areas of nonadherence or gaps in assurance arising from the monitoring of this policy will result in recommendations and proposals for change to address areas of noncompliance and/or embed learning. Monitoring of these plans will be co-ordinated by the group/committee in the monitoring table below.

Element of Policy to be monitored	Lead	Tool/Method	Frequency	Who will undertake?	Where results will be reported?
Transparency – FOI requests	Head of Communications	Report to IMG	Quarterly	Communications Team	IMG

Legal Compliance	Data Protection Officer	Audit, reports, data protection impact assessments	Various	Data Protection Officer	IMG, EMT, Board, SIRO, DSPT
Information Sharing	Information Governance Manager	Audit, reports	Various	Information Governance Team	Caldicott Guardian, IMG, DSPT
Quality Assurance	Information Governance Manager	Audit, reports, procedure review	Various	Information Governance Team	IMG
Breach of Information Security Principles	Information Governance Manager	Data breach reporting	Various	Information Governance Team	Informatics Senior Managers, IMG, DPO, Caldicott Guardian, SIRO, DSPT
Records Management	Information Governance Manager	Audit	Ad hoc	Information Governance Team	IMG, SIRO, DSPT
Education and Awareness	Information Governance Manager	Audit	Annual	Learning and Development/ Mandatory Training	DSPT, IMG, SIRO

13. References

[1] UK Data Protection Act, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf, 2018

[2] EU General Data Protection Regulation, (EU) 2016/679, 27th April, 2016

[3] Records Management Code of Practice for Health and Social Care 2016 , Information Governance Alliance, https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016 , 2016

14. Supporting Documents

The Data Protection & Security Policy is developed as a pinnacle document which has further policies, standards and guidelines which enforce and support the policy. The supporting policies are grouped into 3 areas: Principle Standards, Procedures and User Guidance Documents and are available on the Intranet.

14.1. Principle Standards

14.2. The principle standards detail and explain how information security is to be implemented. These standards cover the approach for elements such as: network monitoring, change control, encryption, access authentication and asset management.

14.2.1. Principle Standards

PS01 Security Responsibilities
PS02 Personnel Security
PS03 Asset Management
PS04 Risk Management
PS05 Third Party Relationship
PS06 Physical Environment
PS07 Access Authentication (Physical)
PS08 Access Authentication (Network)
PS09 Acceptable Use
PS10 Encryption
PS11 Change Control
PS12a Incident Reporting Standard
PS12b Incident Response
PS12c Incident Response (Operational)
PS13 Antivirus and Housekeeping
PS14 Remote Working
PS15 Network Monitoring
PS16 Business Continuity Disaster Recovery
PS17 Monitoring and Audit
PS18 Communications

https://intranet.nwas.nhs.uk/policies-and-guidance/ict-delivery-policies/principle-standards/

14.3. Standards and Guidelines

Standards (mandatory) and guidelines (best practise) will be published separately from this policy to assist ordinary users and system information asset owners to meet their IT Security responsibilities.

14.3.1. Standard and Guidelines

D021 Conditions of Use of Computing & Networking Facilities
D022 Appropriate Use of Computing & Networking Facilities
D023 Computing Auditing Monitoring
D027 Use of Internal email
D028 Use of External email
D029 Use of the Internet
D030 Remote Access
D035 Use of the Intranet
D039 Disposal of Equipment
D044 use Of Anti- Virus Software
D045 Password Management
D049 General Security
D059 Removable Media
D072 Asset Inventories
D073 Email Disclaimer and Storage Limits
D079 Laptop Guidance
D084 Safe Havens
D086 Access Control
D091 Use of Portable Devices and media
D092 Encryption
D093 Acceptable use of IPads

14.4. Procedures

Procedures are split into the following categories:

- Trust wide – for use by all staff
- Department – for use by ICT staff only
- System – these are further categorised for use by the relevant ICT function

These procedures detail the correct way to carry out tasks and are designed to comply with the relevant Trust Information Security standards.

https://intranet.nwas.nhs.uk/policies-and-guidance/ict-delivery-policies/procedures/

Appendix A: Data Protection and Security Strategy

Data Protection and Security Strategy 2019/2020

2018/19will transform the way NWAS protects and secures information through enforcement of the General Data Protection Regulation (GDPR), approval process of the UK's Data Protection Act 2018 and the Care Quality Commission Well Led Key Line of Enquiry now using assurance from the Data Security and Protection Toolkit (DSPT) audit system.

The NWAS Data Security and Protection Strategy for **2019/2020** is to:

1. Embed the systems and procedure changes arising from the GDPR Compliance Project across the Trust.
2. Complete a self-assessment of data security and protection compliance using the DSPT audit tool.

1. General Data Protection Regulation

The General Data Protection Regulation became law in April 2016. It is enforceable from 25th May 2018 and regulated by the Information Commissioner's Office. NWAS will close the GDPR Compliance Project during 2018 which will see significant changes to systems and procedures. The IG Team will lead on embedding these changes across the Trust.

	Responsible	Progress reports to:
Embedding of new systems and procedures	Senior Information Risk Owner	Board
	Data Protection Officer	Board via SIRO Resources via IMG
	Information Governance Manager	Resources via IMG
	Information Asset Owners	IMG

2. Data Security and Protection Compliance Audit

The Data Security and Protection Toolkit is an audit tool developed in response to the National Data Guardian's 2016 review of Data Security, Consent and Opt-Outs and the Government response to the review. The DSPT will be used by NWAS to carry out self-assessment of compliance against the National Data Guardian's 10 data security standards and GDPR.

The IG team will coordinate the completion of mandatory assertions of self-assessment of data security and protection compliance using the DSPT audit tool. The process will be managed in the following way:

	Phase	Responsible	Coordinated by:	Progress reports to:
May 2019 – July 2019	Evidence gathering	Data Protection Officer Information Asset Owners Chief Technology Officer	IG Team	Resources via IMG
August 2019 – October 2019	Internal Audit	IG Team	IG Team	Resources via IMG
November 2019 – January 2020	External Audit	Mersey Internal Audit Agency	IG Team	Resources via IMG
February 2020 – March 2020	Final Submission	SIRO	IG Team	Board via SIRO report