Northern Lighthouse Board		**Q.Pulse Document Number**	OP 41
		Revision number	2
		Implementation Date	1st April 2021
Title	Data Protection Policy		
OP Owner	Data Protection Officer	**Last Reviewed/Update Date**	4th June 2021

Data Protection Policy

1. Introduction

Northern Lighthouse Board (NLB) is required by law to comply with the UK Data Protection Act (DPA) 2018 which came into force on 25 May 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, and the UK General Data Protection Regulations (UK GDPR) 2021 Together they supersede the Data Protection Act 1998 (DPA).

The regulation lays out a framework designed to balance an individual's right to information privacy against the legitimate needs of others to collect and use people's details proportionately in the course of their normal operations (including for the purposes of research, journalism, art, literature and freedom of expression), and avoid causing unwarranted harm.

The right to respect privacy and the right to freedom of expression are considered fundamental to our democratic society. They are both enshrined in the European Convention on Human Rights (ECHR) and incorporated into UK law via the Human Rights Act 1998 (HRA). These are both important rights, and neither automatically trumps the other. UK GDPR protects people's information privacy, but also recognises the importance of freedom of expression, aiming to strike a fair balance.

NLB is committed to ensuring that all employees comply with the DPA and UK GDPR in order to safeguard the confidentiality of all personal data held by NLB regardless of format.

NLB needs to collect, process and retain certain information about its employees and stakeholders in order to allow us to conduct our business operations. In order to comply with data protection law, NLB must ensure that all personal information is collected and used fairly, stored safely, and not disclosed to person unlawfully. In order to achieve this the NLB will comply with the principles of the UK GDPR.

In addition to NLB's primary operational objectives, the organisation has a strong 'family based' culture where the sharing of experience, stories and history are natural and long embedded behaviours. The NLB together with its' staff form an important part of our islands' naval history and as custodians it has collected and maintained records and artefacts which has, and will continue to inform technical, sociological, genealogical and general historical research. In pursuit of this we collect and retain some personal data for the above stated purposes, these cover:

- Articles for the Journal
- Information required for display or research by The Museum of Scottish Lighthouses, the Northern Lighthouse Heritage Trust and the National Library of Scotland
- Oral recollections from former staff members for publication

Much of the information held and artefacts received include Personal Information, this counts as 'processing' and is therefore covered by the UK GDPR.

UK GDPR does not stop us keeping useful information, provided it was obtained legitimately, reviewed from time to time to ensure that it is still up to date (if appropriate), relevant, and deleted when no longer needed. In practice much of our data will be retained indefinitely and archived either in-house or by external bodies such as National Archive Scotland (NAS) and kept to maintain our history and inform future research and publication.

NLB is committed to meeting its obligations under the legislation regarding data protection and confidentiality. Consequences of non-compliance can include reputational damage, loss of public and stakeholder trust, substantial fines, criminal proceedings and claims for compensation against the organisation and individuals.

2. Purpose

The purpose of this policy is to set out NLB's obligations in relation to data protection legislation to demonstrate its commitment to compliance with it. The policy aims to fulfil the requirement for fair and lawful processing of personal data in the records that NLB creates and receives in the course of administering its own business and in the records received and retained for research and/or journalistic purposes.

3. Scope

This policy relates to all staff and applies to all records regardless of format or medium including, but not exclusively, paper, electronic, audio, visual, microform and photographic. It should be read alongside all other appropriate NLB Policies and procedures, listed later in this document.

The UK GDPR replaces the term 'sensitive personal data' with processing of special categories of personal data which is now defined as:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

4. Data Protection Key Principals and Data Retention Schedules

Under Section 193 of the Merchant Shipping Act 1995 the Commissioners of Northern Lighthouses are appointed as the General Lighthouse Authority for Scotland and adjacent seas and islands and the Isle of Man, and under Section 195 are vested with responsibility for the superintendence and management of all lighthouses, buoys, and beacons. In exercising its lawful authority, the NLB carries out tasks in the public interest related to the safety of the mariner at sea; the safety of our own people employed in or around some of the world's most dangerous coastlines; and the safety of environment in which we, and those who come after us, must live and work. NLB Processing of Personal data will primarily fall under four distinct Lawful Bases as defined within the Data Protection Legislation:

Public Task

- Processing of personal data in respect of the exercise of official authority Under Section 193 of the Merchant Shipping Act 1995.

Contract

- Processing of personal data in respect of the performance of our Contract of Employment to which our employees are party; or
- Processing of personal data in respect of taking steps at the request of the Data Subject prior to entering into a contract; or
- Processing of personal data in respect Contracts terms that have been offered and accepted, intended by all parties to be legally binding, in respect of an exchange of goods or services for money.

Consent

The processing of personal data is undertaken only where the unambiguous, evidenced and clearly affirmed consent is held by ourselves. The use of this will be limited within NLB to such areas as sending The Journal to subscribers.

Legitimate Interest

In selecting legitimate interests, NLB take on extra responsibility for considering and protecting people's rights and interests. There are three elements to the legitimate interest basis. We need to be able to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

For example, to fulfil, in part, our duty of care as employees we must ensure that staff who drive vehicles on our behalf hold the appropriate license and are not disqualified. We do not require Consent as we have a legitimate interest.

NLB's primary mechanism for fulfilling our obligation to maintain and demonstrate compliance with data protection legislation is via a framework of Data Retention Schedules. These are owned and maintained at the functional level by a range of Information Asset Owners and will be used to ensure ongoing compliance with Data Protection legislation within NLB's 'business as usual' environment.

Under the UK GDPR, the Data Protection Principles support the Rights of Individuals and set out the main responsibilities for organisations. In respect of the data we process, our Data Retention Schedules will clearly set out the following:

- Lawful basis
- Legitimate purpose
- Data Subject Rights

- Retention Period or rules
- Justification for retention
- Disposal Method
- Information Asset Owner
- Special categories of personal data
- Where appropriate – Consent held

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

No	Principle	Commitment
1	Lawful, fair, transparent	Personal data will be collected and used openly, fairly and lawfully, without causing unjustified harm or intrusion into someone's private life. We will also meet one of listed additional conditions where it is classified as sensitive personal data). These additional conditions are: a. the Data Subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where prohibited by Union or Member State law; 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; 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 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 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; i. processing is necessary for reasons of public interest in the area of public health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; 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)
2	Specific, explicit, for a legitimate purpose	We will clearly identify the specific purposes for collecting all personal data and delineate precisely how we intend to process it. We will define and utilise appropriate and compliant Privacy Statements.

No	Principle	Commitment
3	Adequate, relevant, limited to what is necessary	We will ensure that we hold only enough information to do the job, but not anything we really don't need.
4	Accurate, up to date	We will take reasonable steps to ensure that facts are correct and not misleading, and if an individual disputes them we will investigate and reflect their view. We will take steps in the writing or editing of articles for publication such as in The Journal.
5	Kept no longer than necessary	The regulations do not impose a time limit on retention of personal data. Data Retention Schedules define our retention requirements. Following NLB operating procedures we will delete any details that are no longer needed, retained information is reviewed in line with the organisational policies laid down in our Data Governance Management Framework. The purpose of the review is to ensure that details are still up to date, relevant and not excessive for our needs.
6	Processed Securely	Security policies and procedures operate as laid down in this (and all related documents listed) for both digital and paper based records. These take into account the different types of portable media used to record and store information, including, for example, notebooks, mobile telephones, dictation machines, tablets, laptops and memory sticks.

5. Data Protection Rights of Individuals

The UK GDPR provides for the following rights for individuals:

No	Right	Commitment
1	Be Informed	Where a Subject Access Request (SAR) is made we will provide the information held without obstruction in a concise, transparent, and intelligible manner. It will be written in clear and plain language and supplied to the requestor free of charge. We are required to provide the requested information without delay and at the latest within one month of receipt unless the request is complex we have grounds to extend the period.
2	Access	We will provide confirmation of what personal data are held and being processed, and supplementary information covering how the data has been processed relating this to any applied privacy notices.
3	Rectification	We will rectify inaccurate or incomplete personal data, if we have disclosed the personal data in question to third parties we will instruct them to rectify their records, where possible we will inform the Data Subject of the rectification and we will also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

No	Right	Commitment
4	Erasure	We will in order to prevent processing, on request and unless the right to erasure does not apply , delete personal data where there is no compelling reason for its continued processing if it meets the one or more of the following criteria: • The data is no longer necessary in relation to the purpose for which it was originally collected/processed. • The Data Subject withdraws consent. • The Data Subject objects to the processing and there is no overriding legitimate interest for continuing the processing. • The personal data was unlawfully processed (ie otherwise in breach of the UK GDPR). • The personal data has to be erased in order to comply with a legal obligation.
5	Restrict processing	We will restrict the processing of personal data where the Data Subject; • contests the accuracy of the personal data, until we have verified its' accuracy, • objects to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether NLB legitimate grounds override those of the Data Subject. • opposes erasure, processing is unlawful and requests restriction instead. • requires the data to establish, exercise or defend a legal claim and we no longer need the personal data.
6	Data Portability	We will on request (SAR), and wherever possible, provide the personal data in a structured, commonly used and machine readable form, e.g. CSV files. The right to data portability only applies where: • the Data Subject has provided personal data to a controller; • where our legal basis for processing is for the performance of a contract (such as contract of employment, or based on the Data Subject's consent when • processing is carried out by automated means.
7	Object	Data Subjects may object to processing based on; their legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. Where a Data Subject raises an objection on "grounds relating to his or her particular situation" we will stop processing the personal data unless: • we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or • the processing is for the establishment, exercise or defence of legal claims. We will, via our privacy notice, explicitly bring to the attention of each Data Subject their right to object at the point of first communication, this information shall be presented clearly and separately from any other information.
8	Automated decision making and profiling	The UK GDPR provides the requirement for controls where an organisation: • makes decisions solely by automated means without any human involvement; • automates processing of personal data to evaluate certain things about an individual NLB will not undertake automated decision making or profiling in relation to Personal Data.

Additionally, any exchange of personal information between NLB and International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) will take into account whether an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.
Exemptions exist within the legislation permitting that some requirements do not apply where personal data are processed only for research, statistical, historical or journalistic purposes.

6. Policy Statement & Commitment

In order to fulfil our obligations under data protection law NLB is committed to:

1. Ensuring that Data are processed in line with the Data Subjects Rights including the right to erasure;
2. Making Data Subjects aware when collecting personal data about them, and outlining the ways in which that information will be used through Privacy Statements;
3. Observing fully conditions regarding the fair collection and use of information;
4. Meeting our legal obligations to specify the purposes for which information is used;
5. Collecting and processing appropriate information only to the extent that it is needed to fulfil operational needs, research and journalism or to comply with any legal requirement;
6. Retaining records only for as long as they are needed;
7. Ensuring that people about whom we hold information can exercise their rights fully under the relevant data protection legislation including UK GDPR;
8. Taking appropriate technical and organisational security measures to safeguard personal information;
9. Ensuring that personal information is not transferred abroad without suitable safeguards.
10. Application of exemptions only where appropriate. Specifically in NLB for personal data which are processed only for research, statistical or historical purposes;
11. Compliant, timely, accurate and complete processing of Subject Access Requests;
12. Open and timely disclosure of Data Protection breaches.

This is achieved through:

- The appointment of Director of Business Services Data as the Senior Information Risk Officer; having specific, operational responsibility for data protection in NLB;
- Delegation of ownership and management of the data used in their areas to Information Asset Holders, as set out within NLB's Data Retention Schedules;
- Effective and compliant implementation and utilisation of our key control mechanisms Data Protection Schedules;
- The implementation of appropriate policies, operational procedures and controls;
- The effective implementation of NLB Data Retention Schedules;
- The use of privacy notices to inform Data Subjects wherever collection of personal information takes place, outlining the purposes for which it will be used, who it will be shared with, how it will be securely retained and how individuals may access it;
- Regular oversite of the operation of the policies, controls and operational procedures for the management and security of all NLB records;
- The quick and efficient handling of subject access requests;

- The delivery of training for all NLB staff in information management, security, governance and compliance, to ensure that every member of staff understands their responsibility under data protection law;
- The maintenance of NLB's Data Retention Schedules within the 'business as usual' environment in order to provide verification of destruction as appropriate for all NLB records to ensure information is only retained for as long as it is required;
- Management of data through the SharePoint Electronic Data Management System (EDMS) fully informed by and integrated with NLB Data Retention Schedules.
- The regular monitoring, review and audit via ISO 9001:2008, of the way in which personal information is collected, stored and used by NLB.

Also, where and when appropriate, NLB will:

- Share information in line with the updated Information Commissioner's Data Sharing Code of Practice and establish data sharing agreements with third parties, outlining the terms under which information will be shared;
- Complete privacy impact assessments (as appropriate) in order to assess privacy risks to individuals in the implementation of IT solutions, collection, use and disclosure of personal information;
- Carry out privacy compliance checks to assess compliance with data protection law;
- Actively communicate privacy notices if collecting Special Categories of Personal Data, collecting personal data for unexpected or potentially objectionable purposes, processing information in a way which may significantly affect an individual, or sharing information with another organisation which would be unexpected;
- Include within privacy notices and at other times where personal information may be collected or processed, the Information Commissioner's Information signpost.
- Engage the Information Commissioner's Office directly in policy and process discussions touching on privacy, data sharing and other data protection issues.

The requirement that NLB are able to demonstrate compliance with the legislation will be evidenced through the implementation of the Data Governance Framework.

7. Roles & Responsibilities

Data Protection Officer

The Data Protection Officer has responsibility for identifying and publicising responsibilities for Data Protection within NLB, in accordance with this policy.

The Data Protection Officer is responsible for ensuring that:

- operational Business Information, Personnel Data and Archive Collections are kept up to date,
- processes, Procedures, tools and technology are in place to support all members of staff to comply with their obligations under data protection law,
- guidance and training is issued communication and understood,
- monitoring and reporting to the Audit & Risk Committee ensures the proper functioning of data protection systems,

Information Commissioners Office (ICO) Breach Reporting

NLB Director of Business Services

In the role of Senior Information Asset Owner is primarily accountable for ensuring that all collection and processing of personal data within the organisation complies with data protection law and principles.

Directors and CEO

The Directors and CEO are accountable for the effective implementation of the requirements of the UK GDPR, they regard the lawful and correct treatment of personal information as of vital importance to successful business operations, and to maintaining confidence in our relationships with stakeholders. They will make provision for a regular review of this policy and those associated with it and investigate modifications when necessary.

Senior Managers

As owners of their function based Data Retention Schedules they are accountable for their completion, maintenance and compliance. They are responsible for delegating operational control of Data to Information Asset Holders within their functional area as appropriate.

Information Asset Owners

They are responsible for the completion and maintenance of the Records Retention Schedules for their functions. They are also responsible for oversight and evidencing of the deletion/destruction process.

Line managers

They must ensure that staff with specific data protection responsibilities have these written into their job descriptions and fulfil their data protection responsibilities properly, and that all staff undertake mandatory data protection training.

SharePoint Power Users

Responsible for supporting the Information Asset Owner to ensure that the retention and disposal arrangements detailed within the functional Data Retention Schedules are effectively integrated within the SharePoint system in order to ensure the automation of ongoing compliance with the specified arrangements.

All Staff

All staff within NLB are required to comply with the principles set out in this policy. Breaches of this policy and therefore data protection law may lead to disciplinary action, in line with NLB disciplinary procedures. Colleagues must familiarise themselves with, and follow this policy and the supporting codes of practice, ensure that procedures for the collection and use of personal data is complied with in their area, and familiarise themselves with the implications of data protection in their job by undertaking all appropriate mandatory training, as specified.

8. Legislative Framework

Compliance with this policy will help facilitate compliance with the following acts, regulations and standards:

- Data Protection Act 2018
- EU UK General Data Protection Regulations 2016
- Human Rights Act 1998
- Freedom of information Act 2000
- Freedom of Information (Scotland) Act 2002
- Public Records (Scotland) Act 2011
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

NLB also aims to operate in accordance with the following best practice standards for security and recordkeeping:

- BS ISO 9001:2008 - Quality management systems – Requirements - Certified
- BS ISO 27001:2013 - Information Technology - Security Techniques Information security management systems – Requirements – Certified

9. Documentation

This policy forms part of NLB's overall framework but specifically relates to the following policies and procedures:

- Data Protection Code of Practice
- Information Security Policy
- Clear Desk and Screen Policy as defined in the Information Security Management – 3rd Party Management Manual
- Security Incident Reporting Procedure
- Records Disposal Policy
- Data Handling and Management Policy
- Retention and Disposal Schedule
- Data Retention Schedules
- Use of Privacy Statements
- Standard Contract Clauses