**Data Protection Policy**

**1. Policy Statement**

Protecting the confidentiality and integrity of personal data is a critical responsibility that Seamab takes seriously at all times. We will endeavour to be transparent with individuals whose data is processed and to provide training and support to staff who are handling data so that consistency is achieved. Seamab will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

**2. Purpose of this Policy**

In the course of their work, Seamab staff and volunteers may see or use confidential information about clients, donors, employees, volunteers and others. The General Data Protection Regulation aims to protect individuals’ fundamental rights and freedoms, notably their right of privacy in respect of data processing and access to information held about them. Information can be in both in paper and electronic filing formats including emails, photographs, video clips etc.

The purpose of this policy is to ensure that staff and volunteers do not break the law. If in any doubt about what can or cannot be disclosed and to whom, personal information should not be disclosed until further advice has been sought from individual line managers.

# 3. Scope

This policy applies across the organisation to all staff and volunteers. It is also relevant to our suppliers who may be data processors, and applies to any personal data we may process about external data subjects during the course of our business.

# 4. Principles of GDPR

The Regulation is underpinned by six principles which state that data about someone must be processed with the data subject’s rights at the forefront of activity. Data must be:

* fairly, lawfully and transparently processed;
* processed for limited purposes;
* adequate, relevant and limited to what is necessary;
* kept accurate and up to date;
* not kept in a format where the data subject can be identified for longer than is necessary; and
* secure to prevent the loss, destruction or unauthorised disclosure of data.

In addition, organisations are required to demonstrate compliance with the above.

**5. Key Definitions**

**5.1 Data Processing**

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

**5.2 Personal Data**

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers Seamab possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour.

**5.3 Sensitive Personal Data**

Sensitive personal data is a special category of information which relates to a data subject’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

Personal information may be passed internally from one department to another which reasonably requires it, but this must be done in accordance with the principles of GDPR.

# 6. Lawfulness of Processing

**6.1 Processing your Data**

Depending on how you engage with us, we may process your data for the following legitimate reasons:

* with your consent;
* to fulfil a contract with you;
* to comply with our legal obligations;
* to protect the vital interests of a data subject;
* to meet our responsibilities under the ‘public interest’ requirements; and
* where it is in our legitimate interests to do so, and your rights and freedoms are not negatively impacted.

Various types of processing activity may be undertaken for one or more of the legitimate reasons above. If you ask us about your data, we will tell you which of the above reasons apply. Further details of our legitimate bases for processing your data can be found in our Privacy Policy on our website.

**6.2 ‘Special Categories’ of Data**

Special categories of personal data include the following:

* the racial or ethnic origin of data subjects;
* their political opinions;
* their religious beliefs or other beliefs of a similar nature;
* whether they are a member of a trade union;
* health information;
* genetic or biometric data used to identify a data subject; and
* data about sexual orientation or sex life.

We will only process this type of data about you in the following circumstances:

* with your consent;
* to meet our obligations under social security, employment and social protection law;
* to protect the vital interests of a data subject if they are unable to give us their consent;
* in accordance with our legitimate activities in relation to our purposes as a charity, where we will not share the information with third parties without your consent;
* where this information has already been made public by you;
* in defence of legal claims;
* where there is substantial public interest benefit;
* for purposes of occupational health, assessment of working capacity of an employee, or for the provision of health and social care services;
* where there is a public health reason; and
* for archiving, research or statistical purposes.

#

# 7. Responsibilities

The Board of Trustees has overall responsibility for ensuring the organisation complies with legal obligations under the legislation.

Seamab is a Data Controller under the GDPR. The Data Controller is responsible for ensuring that necessary steps are taken to ensure compliance with the Regulation.

The Chief Executive/SMT has responsibility for ensuring that the charity maintains day-to-day compliance with the legislation and for reporting any breaches to the Information Commissioner.

The Finance and Administration Manager has responsibility for ensuring that our electronic systems are maintained in line with the legislation.

All staff and volunteers are required to read, understand and accept any policies and procedures relating to the processing, recording and storage of data about individuals that the charity supports. Staff also have a duty to report any data breaches in line with the Data Breach procedure. Breaches of the Data Protection policy may be dealt with under the organisation’s disciplinary procedures.

All staff are required to be aware of the Freedom Of Information (Scotland) Act (FOISA) and Environmental Impact Assessment Regulations 2017 (EIR), the obligations it puts on Seamab School as a public authority, and how to deal with any such request.

In general, access to personal information will be dealt with as a subject access request by the HR Manager and the Head of Service. In limited cases personal data may be disclosed under FOISA - the HR Manager can provide guidance on which legislation applies.

# 8. Your Rights

As a data subject you have the following rights when we process your data (see our privacy notice for full information):

* the right to be informed about how we process your data;
* the right to access information we process about you – see the next section on ‘subject access requests’;
* the right to rectification;
* the right to erasure;
* the right to restrict processing;
* the right to data portability;
* the right to object to us processing your data; and
* rights in relation to automated decision making and profiling.

# 9. Subject Access Requests

**9.1 Individual Access to Data**

Individuals have the right to access data held about them under a ‘subject access request’. Such requests will be dealt with by the HR Manager and the relevant Head of Department.

Any such request must be made in writing. A copy of this policy and a Subject Access Request Form may be sent to anyone making such a request. The charity will acknowledge receipt of a request in writing and set a date by which the request will be fulfilled. The charity must respond without undue delay, and within one calendar month.

In accordance with the regulation, Seamab will provide the following information:

* whether or not we process any data about you;
* the purposes of the processing;
* categories of data processed;
* categories of third parties with whom we may have shared your data with;
* retention information;
* where we obtained your data (if not obtained from yourself) – if we know this;
* any use of automated decision-making on your data; and
* if your data has been transferred overseas and how we protected it.

We can provide you with a copy of your personal data undergoing processing, and this will usually be supplied electronically. Supervised access to Seamab’s premises to access the relevant records may be granted if appropriate. The data subject must satisfy Seamab of their identity prior to information being released.

**9.2 Rectification and Erasure**

Should any of the data we hold about you be inaccurate, you have the right to request that we rectify it and we will do so without undue delay. In certain circumstances you also have the right to request that we stop processing your personal data, and we will do this without undue delay if this is appropriate. Please note that there are some exemptions to this right and Seamab will inform you as to our ability to meet this right should you choose to exercise it.

# 10. Privacy and Electronic Communications Regulations (PECR)

Seamab’s fundraising and marketing activities include electronic communications (e.g. email, phone, text and social media) with supporters. We comply with the PECR alongside the GDPR. We obtain consent for our fundraising/marketing communications and have a valid privacy notice on our website. Our supporters may opt out of receiving marketing information at any time. We are clear on our use of cookies and have a statement explaining this.

# 11. Data Recording and Storage

Data on any individual will be recorded in as few places as possible, and duplication of data sets is discouraged. Procedures to ensure that all relevant systems are updated when personal information changes will be regularly reviewed.

Seamab has developed a document retention schedule as part of the Records Management Policy and this should be referred to when records are being stored or are to be archived.

The GDPR expects anyone handling personal information to protect it and ensure that it is not lost, stolen or misused. Should any information be lost, this may be reportable to the Information Commissioner’s Office.

# 12. Use of Portable Devices to Record and Transport Electronic Data

Our IT Policy contains guidance on our policies on use of mobile phones and other portable items.

# 13. Consent

Seamab’s privacy notice can be found on our website. We will ask people’s permission to use their data for specific purposes, e.g. communications about organisational activities, and send an ‘unsubscribe’ option with every such communication.

Seamab acknowledges that consent to use certain information can be withdrawn at any time. This will apply from the date of receipt of such notification and cannot be backdated. There may be occasions where it would be necessary to retain data for a specific period of time, even though consent for using it has been withdrawn. The organisation will respect the rights of the individual in this regard, unless doing so would endanger the person concerned.

# 14. Procurement/Data Processors

Whenever a data controller uses a processor to process data on its behalf, a written contract needs to be in place, which will define responsibilities and liabilities. We will only appoint processors who can provide ‘sufficient guarantees’ that the requirements of the GDPR will be met and the rights of data subjects are protected.

The GDPR imposes restrictions on the transfer of personal data outside the European Union. Personal data may be transferred outside of the EU if appropriate safeguards are in place, as defined by the Information Commissioners Office (ICO) on their website. Seamab contracts with data processors who are either based in the EU or provide adequate evidence of the safeguarding of our data in line with ICO requirements.

Our standard terms and conditions contain clauses relevant to Data Protection.

**15. Data Sharing**

Seamab requires third parties to respect the security of personal data and to treat it in accordance with the law. Seamab may share personal information with third parties where it is necessary to administer the working relationship with employees or where Seamab has a legitimate interest in doing so. Seamab may also need to share personal information with a regulator or to otherwise comply with the law.

If using third party processors, e.g. for bulk mailing or database management, and giving them access to personal information, there must be a written contract in place with them to ensure that the third party treats the information confidentially, securely and in compliance with GDPR.

Staff must not share any data relating to other staff members, volunteers or children outwith their Seamab duties. It is not acceptable to store any photographs of children on personal devices. Staff must ensure that personal photographs do not contain any images of children, identifiable or not.

**16. Review of Policy**

This Policy will be reviewed regularly and if there are any material changes to legislation and guidance.