DATA PROTECTION POLICY

Written by	Ryan Beasley, Executive Officer
Date submitted	August 2022
Approved by which forum	Executive Committee ☐ Trustee Board ☒
Date of approval	
Last date of renewal/review*	
Next date of renewal/review*	

All policies should be reviewed every three years unless stated otherwise.

INTRODUCTION

BELMAS handles personal data of individuals on a regular basis as part of its operational requirements. These individuals can include: members of the organisation, business contacts, suppliers, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet with the organisation's data protection standards – and to comply with the law.

For further information about this policy please contact the Executive Officer Union at info@belmas.org.uk

AIMS

This data protection policy ensures that BELMAS:

- Complies with general data protection regulations, the law and follows good practice;
- Protects the rights of staff, members and partners;
- Is transparent about how it stores and processes individuals' data; and
- Protects itself from the risks of a data breach.

SCOPE

This policy applies to:

- The Board of BELMAS;
- All staff and volunteers of BELMAS; and
- All contractors, suppliers and other people working on behalf of BELMAS.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers; and
- … plus any other information relating to individuals

What is personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Special category data

The GDPR calls personal information that is particularly sensitive 'special category data'. This includes:

- Race;
- Ethnic origin;
- Politics;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life; or
- Sexual orientation.

BELMAS recognises that these sensitive pieces of information and will take extra care when using or processing them in accordance with this policy.

Data protection law

The General Data Protection Regulations 2018 describes how organisations – including BELMAS – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles of the GDPR. These say that personal data must:

1. **Lawful, fair and transparent**

   There has to be legitimate grounds for collecting the data and it must not have a negative effect on the person or be used in a way they wouldn't expect.

2. **Limited for its purpose**

Data should be collected for specified and explicit purposes and not used in a way someone wouldn't expect.

3. **Adequate and necessary**

It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected.

4. **Accurate**

Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.

5. **Not kept longer than needed**

Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.

6. **Integrity and confidentiality**

Data should be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, loss, damage or destruction, and kept safe and secure.

Under the GDPR, data subjects have a number of rights regarding the use of their personal information. They can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Risks and responsibilities

Data protection risks

This policy helps to protect BELMAS from data security risks, including:

- Information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information; or
- Individuals being harmed through data being inaccurate or insufficient.

An inventory of the GDPR risk areas and specific data sets within BELMAS is outlined in **Appendix 1: Inventory of Data Sets** of this policy.

All retention policies specifically for accounting and personnel/employee records can be found in **Appendix 2: Retention of Accounting and Personnel Records.**

Data controller and data processor

According to Article 4 of the EU GDPR, different roles are identified as indicated below:

Data Controller – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determine the purposes and means of the processing of personal data"

Data Processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

BELMAS is a data controller.

BELMAS will only process personal data where it has a lawful basis for doing so. It will only process special category data where it has an exception to do so.

Where the lawful basis or exception is 'consent', it will be stored the same length of time as the personal data.

Responsibilities

Everyone who works for BELMAS has some responsibility for ensuring that data is collected, stored and handled appropriately, and everyone who handles such data must ensure that it is processed in line with this policy and the six principles of GDPR.

BELMAS (Data Controller)	The Board of Trustees have overall responsibility for ensuring that the organisation complies with its legal obligations.
Executive Officer (Data Protection Officer)	The Executive Officer as the most senior member of staff has the responsibility to: • Brief the Board on Data Protection responsibilities; • Review Data Protection and related policies; • Advise staff on all Data Protection issues; • Ensure Data Protection induction and training takes place; • Handle subject access requests; • Approve unusual or controversial disclosures of personal data; • Ensure that good Data Protection practice is established and maintained across the organisation; and • Ensure that all staff and volunteers follow the BELMAS Data Protection Policy.
Staff and Volunteers	All staff and volunteers are required to read, understand, acknowledge and accept any policies and procedures relating to personal data that they may handle in the course of their work.
Enforcement	Individuals found in breach of this policy may be subject to disciplinary procedures.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from the Executive Officer.
- BELMAS shall provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines under the "Data storage" section of this policy. In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- Data should be reviewed regularly and updated (recommended bi-annually for each area). If it is found to be out of date, or no longer required, it should be deleted and disposed of.
- Employees should request help from the Executive Officer if they are unsure about any aspect of data protection.

Data recording and storage

Storing data electronically

When storing data electronically all staff must:

- Ensure that the data is protected by strong passwords that are changed regularly.
- Ensure that any data stored on removable media such as CD, DVD should be kept locked away securely when not being used. Memory sticks should be encrypted and password protected;
- Data should only be stored on designated drives and servers. For the purpose of BELMAS, this means their password protected user area or the shared drive (P:Drive) which only BELMAS staff have access to;
- Data should never be saved directly onto laptops or other mobile devices like tablets or smart phones, unless they are BELMAS property protected by approved security software and a firewall;
- Transfer data from emails immediately onto relevant and appropriately secured documents. All emails should be deleted when no longer required, or archived appropriately and securely;
- Encrypt confidential information in accordance with **Appendix 3: Encrypting Confidential Data when Sending via Email;**

- Ensure that the screens of their computers are always locked when left unattended. Staff can also request for a computer visibility screen by contacting the Executive Officer;

- All servers and computers containing data should be protected by approved security software and a firewall. For the purpose of BELMAS, they shall only use servers provided by BELMAS IT partners with installed security software and firewall;

- Ensure that data will be held in as few places as possible to prevent duplication of data sets;

- Update data as soon as inaccuracies are discovered. For example, if a partner can no longer be reached by their telephone number, it should be removed from the database.

Storing data on paper

When storing data on paper all staff must:

- Ensure that it is kept in a secure place such as in a locked drawer or locked filing cabinet;

- Ensure that data is not left unattended where unauthorised people could see them, such as on a desk or on a printer; and

- Ensure that all data printouts are shredded and disposed of securely when no longer required.

Recording data

When recording data all staff must:

- Ensure that the information is correctly recorded. If information is being taken by phone, staff must repeat the data back to the individual if in a secure office, or alternatively follow up with an email to confirm the information is correct;

- Annually contact all individuals who the organisation holds data about to ensure that all data is up-to-date; and

- Contact any individual who has had their data given to BELMAS by a third party organisation to inform them how and why BELMAS has their data, and where appropriate, to check its accuracy.

Data subject access request

All individuals who are the subject of personal data held by BELMAS are entitled to:

- Ask what information the company holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up-to-date; and
- Be informed how the company is meeting its data protection obligations.

If an individual contacts a company or organisation requesting this information, this is called a data subject access request.

Data subject access requests are the responsibility of the Executive Manager on behalf of the Board of Trustees. The Executive Officer shall handle the subject access request **within the legal time limit of one month.** You can read more about data subject access requests on the Information Commissioner's website https://ico.org.uk/for-the-public/personal-information/

Requests should be made to the Executive Officer via the shared inbox at info@belmas.org.uk

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, BELMAS will disclose requested data. However, the Executive Officer will ensure the request is legitimate, seeking assistance from the Board of Trustees and from the organisations legal advisors where necessary.

Data sharing agreement

BELMAS shall have a data sharing agreement with SAGE Publications that outlines the purpose of sharing the data for the purposes of accessing BELMAS owned journals online.