Appendix 1: Inventory of data sets

BELMAS commits to conducting good practice in data protection. As part of this, we recognise where it holds data and makes annual assessments on:

The risks attached to the data set or storage area;

How the data set is stored;

Whose responsibility it is to ensure that the data is safe and secure; and

What the retention policy is on the specific data set.

Below is an inventory of the risks for areas where specific data sets may be held by BELMAS process. For the purpose of this inventory "Staff" means BELMAS Staff, Officers and Volunteers.

Data / risk area	Specific risks	Storage/security/precautions	Responsibility	Retention period if applicable	Reason for retention period
BELMAS papers for meetings	Staff leaving meeting papers on their desks.	All papers should be filed correctly. Paper copies are stored on the shelf in its relevant folder and electronic copies shall be stored on the P:Drive. Any paper copies with confidential information should be stored in a locked filing cabinet.	All staff.	All meeting papers stored physically or electronically shall be deleted or destroyed appropriately after 5 years.	For historical context of future meetings.
	Papers not being collected from the post.	The post should be collected from the Acero Spaces desk on a weekly basis.	All staff.	N/A	N/A
Employee/ personnel records	Employee/personnel records are viewed by an inappropriate person.	Employee/personnel records are ONLY handled by the Executive Officer and HR and Finance Officer.	Executive Officer. HR and Finance Officer.	The retention of all employee/personnel records shall be stored in accordance with the Retention of Accounting Records as described in Appendix 2.	SEE APPENDIX 2.

		All staff contracts have a section on confidentiality and the individuals handling this data are expected to adhere to this.			
Accounting records	Accounting documents and records are viewed by an inappropriate person.	All accounting documents and records should be stored in a locked cupboard or filing cabinet and access restricted to relevant staff.	Executive Officer. HR and Finance Officer.	All accounting documents and records are to be destroyed in accordance with the retention of Accounting Records as described in Appendix 2.	SEE APPENDIX 2.
Staff emails, computers and other office equipment	Staff leaving computers unattended.	All computers are to be locked when staff leaves their desk. This includes while home working, remote working and working in shared spaces.	All staff.	N/A	N/A
	Staff leaving emails logged in to shared computers.	All staff should log out of their email addresses before shutting down any computer. Staff should never, under any circumstances, auto-save their usernames or passwords on a shared computer.	All staff.	Emails that are no longer required should be deleted immediately.	No longer required.

		All staff should keep on top of their emails, archiving appropriately.		All emails that are older than 12 months but are still required should be archived onto the P:Drive or the user area.	Good practice for secure information storage.
	Staff having confidential phone calls in a busy office.	Staff are expected to ensure that all confidential calls are made in a quiet and private location. If this is not possible at home, the Executive officer can make arrangements for a temporary office space.	All staff.	N/A	N/A
	Staff working on documents which have data sets on a computer within a busy shared office.	While staff work from home, they may from time to time work in public spaces. Staff can request a privacy screen from the Executive Officer for these occasions.	All staff.	N/A	N/A

	Former members having access to passwords and emails after they leave their post at BELMAS.	All passwords for emails accounts, social media accounts and other electronic accounts should be changed annually/regularly.	All staff.	N/A	N/A
BELMAS website and other websites	Data subjects input their data into forms on the website which can be accessed if the website is hacked, or if previous members of the team have log in details.	User log-in passwords for the BELMAS website should be changed annually. All staff should be vigilant of any unusual activity on the BELMAS website and report anything immediately to the Executive Officer who will seek assistance from our IT providers.	All staff.	Forms no longer used by BELMAS on all websites should be deleted immediately.	No longer required.
	Data subjects information no longer up-to-date on the BELMAS website.	Staff should check annually with members that the information we hold for them is correct.	Executive Officer.	Data sets no longer required by BELMAS should be deleted immediately on the back end of the website.	No longer required.

Data sharing agreement with external parties	Members are not aware of the external partners BELMAS works with.	BELMAS should be transparent to the membership, being clear what websites and partners it uses when annually reviewing member information.	Executive Officer	N/A	N/A
Marketing and partner lists	Marketing and partner mailing lists are out of date.	BELMAS will contact all data subjects annually to check: 1. What information BELMAS holds 2. That the information held is correct; and 3. An option to "opt-out" or remove their data from the database.	Executive Officer	All data should be checked regularly and amended 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. Annual formal checks.	Inaccurate information is no longer required.

	Marketing and partner data subjects are not aware of how to opt out of BELMAS marketing	BELMAS will contact all data subjects annually to check: 1. What information BELMAS holds 2. That the information held is correct; and 3. An option to "opt-out" or remove their data from the database.	Executive Officer	Annually.	Good practice for keeping data sets up-to-date.
All data stored on the BELMAS Shared drive (P:Drive)	Inappropriate individuals gaining access to the BELMAS (P:Drive).	Only personnel with staff contracts shall have access to the P:Drive which will be communicated with our IT providers. Access shall be removed for staff within 1 week of them leaving BELMAS.	Executive Officer	N/A	N/A