Beds SU Data Protection Internal Audit Report

February 2023

1. Introduction

An audit has been carried out to assess Beds SU'sSU's management of personal data in accordance with General Data Protection Regulation (GDPR) which came into force in May 2018 and is regulated in the UK by the Information Commissioner Office (ICO).

GDPR sets out rules regarding the managing, handling, and utilising of personal data. It provides a legal framework for keeping everyone's personal data safe by requiring companies to have robust processes in place for handling and storing personal information. This framework is guided by seven key principles, which cover the following:

1. Lawfulness, fairness, and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality (security)
7. Accountability.

Beds SU utilises personal data for many different reasons, including staff administration, managing members' rights to representation & democracy, providing advice service, communicating with members, monitoring equality and inclusivity, managing purchases etc. It is important to ensure that the utilisation of personal data accords with the requirements of the data protection act across all services.

An audited assessment of data protection practices was carried out across each Beds SU department area, grouped as follows:

- Representation
- Advice and Enquiries
- Marketing and Communications
- CEO and Exec Officer
- HR, Finance and Commercial services
- Societies and Student Groups

This report outlines the outcomes of these assessments, highlighting any risks, action to be taken and further recommendations.

2. Compliance

The following regulated compliances are in place

- **Data Protection Policy** – Updated in Feb 2022, all documentation is accessible via the Beds SU website www.bedssu.co.uk/Data-Protection. This policy and associated procedures are reviewed every two years and approved by the SLT, and then ratified by the Board of Trustee

- **Privacy Notice** – Updated in Feb 2022, and is available via the Beds SU website www.bedssu.co.uk/data-protection/privacy
- **ICO registration** – Beds SU is registered with the ICO with the following certification:
    - **Registration reference:** ZA286918
    - **Date registered:** 17 November 2017
    - **Registration expires:** 16 November 2023
    - **Payment tier:** Tier 1
    - **Data controller:** Beds SU

3. Enforcing Data subject rights

Access to information:

- Student data subjects can access much of the information Beds SU holds on them via login into the Beds SU website. Alternatively, they can contact Beds SU
- Staff data subjects can access much of the information Beds SU holds on them via two main HR systems. This is Bright HR for permanent staff and Staff Savvy for student/casual staff
- All other data subjects can contact Beds SU for access to information held about them.
- If a data access request involves providing a release of any data Beds SU holds of a data subject, making changes to data, or making a complaint, they will be required to complete a Data Subject Request Form, available here: https://bedssu.forms-eu.com/view.php?id=75136

How to get in contact: All data and information requests should be sent by email to help@bedssu.co.uk and will be handled by the Data Protection Lead.

Data Protection Lead: The Data Protection Lead for Beds SU is the Mark McCormack (CEO). Data Protection Lead responsibilities are currently devolved to Lisa Roerig (Head of Marketing, Communication and Business Development)

4. Data sharing agreements and New Processing of data

All data sharing agreements in place in February 2022 can be found in Data Protection Policy Appendix: Data Sharing document: https://bed-cdn.ams3.digitaloceanspaces.com/resource/5aLCnu7ZPMzQ5it1rIIWCh9A7xaSsJzm1GgiQuAL.pdf

Any additional Data sharing agreements after this time are outlined and approved in a Data Protection Impact Assessment (DPIA) and highlighted in the organisation's Data Protection Audit.

New data processing of personal data approved via DPIA in this period are

- Freshdesk
- MemPlus
- LearnWorlds

5. Breaches

Beds SU did not recorded any data breaches since its last audit.
It was reported that a staff laptop was stolen; however, due to robust data security measures in place, this was regarded to pose a low to no risk to data subjects.

6. Staff Awareness

Staff should complete the following before they are granted access to data held by Beds SU:

- Complete and pass a Data Protection/GDPR online course via the university-provided WorkWise OLAS system
- Read the Beds SU Data Protection Policy and appendix documents
- Review a presentation on Beds SU data protection procedures
- Complete a Data Protection Declaration.
-

Staff are required to also complete and pass the WorkWise OLAS Data protection course on an annual basis.

Staff can seek ongoing advice and guidance from the appointed Data Protection Lead

Data breaches or concerns are to be reported to the Data Protection Lead or a member of SLT as soon as possible and within 48 hours. A data breach record form will also need to be completed.

7. SLT awareness and accountability

The Data Protection Lead reports to SLT on all issues arising regarding data protection.

SLT is responsible for the following:

- Approval of Policy and Procedures, which is then ratified by the charities board of trustees.
- Approval of DPIA and adoption of new processes involving personal data
- Recording beaches and implementing measures to further irradicate risks

8. Audit Summary

This audit highlights Beds SU's strong commitment to data protection and ensuring the right of individuals are upheld.

- Mechanisms are in place to ensure it adheres to the seven principles of GDPR.
- Every effort is made to ensure data subject understands and agrees to how their data is used and managed.
- Personal data is only processed for legitimate purposes and in accordance with our data protection policies.
- Data subjects are made aware of how they can access data collected about them.
- Retention periods are in place for all personal data help, albeit some of these processes are currently manual.

- Adequate security measures are in place to ensure data is secure.

9. Key areas of consideration

The following is a list of the potential risks identified in each departmental audit.

Business Area	Risk Identified	Level of risk (High, Medium, Low)	How can this or is this being managed:
Societies and Student Groups	Unauthorised access to computers	Low	Staff to ensure computers are always locked when unattended
	Ensuring the deletion of personal data on the Society data spreadsheet takes place in line retention policy – this is currently a manual process.	Medium	New academic year preparation to include data replenishment actions
	Student Committee member access to data – misuse of data, breach of policies and/or GDPR reg	Medium	Annual training, presentation and data declarations must be signed before access is granted. Committee members only have limited access to data, as required to run activities.
HR Finance and Commercial	Archived hardcopy file management. The risk of loss of data.	Low	Secured in lock units. Files are being moved online, and hardcopies destroyed ASAP
Representation	The retention period of Student Rep spreadsheet data is currently manually managed	Low/Medium	Personal data is removed after five years as per the retention policy. Appointed staff member to update

			system annually and part of new year actions plan
	Shared password for LearnWorlds	Low	Change password annually, and when someone leaves the team
Communications	Paper permission forms and sign-up – risk of misplacement	Low	To be administered online or scan, and paper copies destroyed as soon as this is possible
	Protection of high volumes of personal data within Memplus and Machforms	Low	Data protection sharing agreement provider. Secure systems in place. Individual staff access via password and 2 step verification where needed. Staff declaration in place before access given. Retention processes in place
	Not all computer anti-virus software being up to date	Medium	Access to data facilities removed until staff members confirm up to date software is installed
Advice and enquires	Freshdesk Adhering to retention period policy currently a manual process	Low	Request auto delete after 5 years from Freshdesk if possible – Data has not yet met this threshold
	Data cross pollination – use of previously completed forms send to new enquiries	Medium	Additional training for staff as required Using the systems provided as intended to mitigate risk

10. Action Log

The following are actions that are required under each departmental audit to improved system and processes and ensure ongoing compliance.

Action:	Responsibility:	Completion Date:
Investigate race, gender and disability coming from SITs records, so this no longer needs to be collected separately	Amy	June 2023
Investigate a mandatory tick box to be in place on Freshdesk forms to indicate consent related to Privacy Statement. Wording to be adjusted to indicate "submit from" implies it this if the tick box cannot be provided	Amy/Candy	End of March 2023
Freshdesk – Investigate auto delete of data after five years and add privacy notice to automated email acknowledgement	Amy/Candy	June 2023
Investigate Advice Pro exporting data record to .CSV	Amy	End of March
Ensure Exec complete data protection declaration	Mark/Ann	ASAP
CleanMyMac to be added to all MacBook'swithin team	Cass	Mid Feb 2023
DPIA to be approved by SLT and noted for the next Data Protection policy review for Memplus	Lisa	Mid Feb 2023

Disclaimer data protection notice to be provided on Airtable	Amy	Mid Feb 2023
Airtable & LearnWorld DPIA needed	Amy	Mid Feb 2023
Student Staff Data Protection agreement to be updated and signed in line with permanent staff agreement	Ann	End Feb 2023

11. Further Recommendations

- **Record retention** – In several instances data retention periods are being managed manually. This poses a risk of the deletion of data not being carried out once is no longer required. Beds SU should seek automatic solutions wherever possible to reduce this risk.
- **New software/collecting/processing approval process** – It is noted that DPIA are not being completed and approved as a matter of course before the implementation of a new ways of collecting and/or processing of personal data. It is recommended that SLT reinforce this and ensures required due diligent is taken to ensure GDPR compliancy are in place before use.
- **Update to staff presentation** – In line with the update of the Data Protection Policy it is recommended that Beds SU reviews it current presentation to staff for to ensure all information is up to date.
- **Awareness of new data processes** – Data subject should be made aware of any new ways of processing their data. If a new system is introduced, this should be approved via a DPIA and shared with the data subject. This could be at point of access of via a new section on the Beds SU Data Protection website pages, highlighting any new processes outside that already recorded in the last data protection policy review.

12. Next internal data protection audit

This should take place no later than March 2025