J-SOC DATA PROTECTION GUIDANCE

INTRODUCTION

The Union of Jewish Students has created the following data protection guidance document to support and enable all J-Socs to follow GDPR practices as best as possible. This document describes how personal data must be collected, handled and stored to comply with the law. As a J-Soc, different types of information may be gathered and stored to contact and recruit students for events, initiatives and trips.

This includes:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals (dietary requirements, access needs, events previously attended etc..)

Examples of Good GDPR Practice

- Only storing information that is needed (in order to recruit and reach out to students)
- Storing personal information such as phone numbers, names and addresses in safe places (lockable drawers, secure laptops)
- Shredding and disposing of confidential information when no longer needed
- Only relevant committee members should be able to access the data held
- Data should not be shared informally or externally in any format
- Emails to more than one individual should be put out using 'BCC'

Examples of Poor GDPR Practice

- Leaving notes or personal information in public places
- Sharing of personal information to anyone outside of the committee
- Breaches of confidentiality- e.g. information being given out inappropriately
- Failing to offer choice – all individuals should be free to choose how their information is stored
- Using the data for other reasons besides the J-Soc

All J-Soc members have an obligation to report data protection breaches to UJS (info@ujs.org.uk) if they have concerns of such a breach. This will allow UJS to investigate further and take appropriate steps to fix the issues in a timely manner.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by J-Socs are entitled to:

- Ask what information the J-Soc holds about them and why
- Ask how to gain access to it
- Be informed how the J-Soc is meeting its data protection obligations.

If an individual contacts the committee and requests this information, this is called a subject access request. Subject access requests from individuals should be made in writing or by email, Twitter or Facebook. The J-Soc should then aim to provide the relevant data within a calendar month.

The committee should ask UJS if they are unclear about any aspect of data protection.

Further information on GDPR can be found on https://www.ujs.org.uk/privacy