Data Security Policy

1. **Context:**

    a) This policy set outs the organisations policy, practices and processes in order to ensure the security of electronically held data.

    b) The policies, practices and processes to ensure the security of non-electronically held data is outlined in the data storage policy and this should be used as the guiding policy for such matters.

2. **Main Organisational Network:**

    a) As the Union uses the main University network to ensure data security our employees and volunteers will be bound by and follow any non-conflicting elements of the following University policies and procedures when using the University network to ensure data security and promote best practice;

        i. Anti-Virus policy
        ii. Bring your own device policy
        iii. Data Security Policy
        iv. Interception Policy
        v. Network Acceptable Use Policy
        vi. Network Password Policy
        vii. Software Licencing Policy
        viii. Use of mobile telecommunications

    b) In addition to following the above policies and procedures the Union works actively with the Universities ICT team through the following mechanisms to ensure data security:

        i. The Union is a member of the Universities ICT strategy committee where data security members are discussed and agreed.

        ii. The Union actively participates in University initiated penetration testing and actively responds to any actions raised following such testing.

        iii. The Union actively participates in University internal data security audits and actively responds to any actions raised following such audits.

        iv. The Union uses the Universities service desk to report and gain support on any ICT incidents or issues.

3. **Third Party Software and Cloud Storage and Servers:**

a) Before contracting, engaging with or using any additional third-party software, cloud storage and servers the Union will undertake due diligence and gain appropriate assurances that;

i. The provider is completely compliant with the General Data Protection Regulations (GDPR).

ii. The provider operates under industry standard data security measures and has appropriate data security policies and procedures in place.

iii. The provider has appropriate security testing and incident logging in place to manage security risks.

iv. The Union has a comprehensive and complaint data sharing agreement in place signed by authorised individuals.

v. The Union has undertaken a comprehensive Data Impact Assessment (DIA) that has been approved by the Senior Leadership Committee.

vi. The responsible department has effectively updated its departmental risk assessment which has been approved by the relevant senior manager.

4. Key Union Policies:

a) This policy should not be read in isolation as the following Union policies contain critical information, policy and operational procedures to ensure adequate management of data security;

i. Data Storage Policy
ii. Data Protection Policy
iii. Privacy Policy
iv. Data Retention Policy
v. Data Breach and Reporting Policy

5. Staff Development & Training:

a) Upon induction, in the organisation, all employees are given clear guidance and knowledge of the policies and procedures the organisation has.

b) All staff are required to complete an online data protection training module alongside passing an online test in relation to data protection and security.

c) All staff are required to complete an online training module covering the principles and individual rights in relation to the General Data Protection Regulations (GDPR).

d) Data protection and security development for relevant staff members are continually reviewed by relevant line managers and where appropriate additional training and continued professional development is put in place.

e) Any changes to data protection or security-related policies will be followed by a face to face briefing workshop to explain changes that have been made.

f) Should any changes to data protection or security law and regulations occur these will be clearly communicated and explained to the staff at a relevant staff conference event.

6. Review:

a) This policy will be reviewed as minimum every two calendar years but sooner if;

i. A relevant change in law or policy occurs
ii. A data breach takes place internally
iii. A data breach takes place with one of our providers

Policy Number:	**Approving Body:**	**Date Ratified by Board:**	**Renewal Date:**
30.V2	Senior Leadership Team	October 2018	October 2020