Data Security Breach Policy

1. Policy Aim

1.1. The aim of this policy is to ensure that the response that York St John Students' Union takes to any reported data breach incident is efficient and effective and ensure that any breach is appropriately logged and managed in accordance with best practice guidelines. By adopting a standardised consistent approach to all reported incidents, the Students' Union aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- incidents are recorded and documented
- the impact of the incidents is understood, and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

1.2. The Students' Union holds data / information, both in hard and soft copy. This includes personal or confidential information (about people), and non-personal information which could be sensitive or commercial, for instance financial data, performance reviews and similar information. Care should be taken to protect this type of data / information, to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands, that its authenticity and integrity is maintained. In the event of a breach, it is vital that appropriate action is taken to minimise associated risks.

2. Definition of a breach

A data breach is an incident in which data is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples include:

- Accidental loss, or theft of equipment on which data is stored or of the paper copies
- Unauthorised access to data
- Human error such as emailing data by mistake
- Failure of equipment and hence data held on it
- Loss of data or equipment through fire or flood, for instance
- Hacking attack
- Where information is obtained by deceiving a member of staff

3. Reporting a data breach

Data security breaches should be reported immediately to the Chief Executive Officer. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved.

4. Investigation of a breach

The Chief Executive Officer, or his/her designate, will instigate an investigation. The investigation should commence within 24 hours of the breach being discovered (where this is not possible, then as soon as the potential breach is known). The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals, and if so, who are the subjects and how many are involved. The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to the Students' Union.

5. Containment, recovery and future review

5.1. Following an investigation, the Chief Executive Officer will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down equipment. Appropriate steps will be taken to recover data losses and resume normal business operations. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords. Advice from experts in the University or from external organisation with relevant expertise may be sought.

5.2. Once the breach is contained a thorough review of the event will be undertaken by the Chief Executive Officer, to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible after consultation with the Trustee Board.

6. Notification of the breach

The Chief Executive Officer will decide based on the seriousness of the breach whether or not to notify the Trustee Board. The Chief Executive will also decide to inform any external organisation, such as the police or other appropriate regulatory body particularly the Information Commissioner's Office (ICO). If a personal data breach has occurred, or a breach defined as a 'notifiable breach' this will be reported to the ICO within 72 hours of the Chief Executive Officer becoming aware of the breach. Failure to do so can result in a significant fine or action. Notice of the breach will also be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks into the future.