



North Northants Social Enterprise Network

connecting, supporting, promoting

NNSE Data Breach Policy

NNSE is committed to protecting the privacy and security of all personal and sensitive information collected and processed in the course of its activities. This Data Breach Policy outlines the procedures for identifying, responding to, and mitigating data breaches within NNSE.

- The purpose of this policy is to:
 - Define a data breach and provide examples of potential breaches.
- Establish procedures for detecting, reporting, and responding to data breaches.
- Minimize the impact of data breaches on individuals and NNSE operations.
- Ensure compliance with data protection laws and regulations, including the General Data Protection Regulation (GDPR).

This policy applies to all NNSE members and volunteers and any third parties who handle personal or sensitive information on behalf of NNSE.

A data breach is defined as any unauthorised access, disclosure, alteration or destruction of personal or sensitive information that compromises its confidentiality, integrity, or availability.

Examples of data breaches include:

- Unauthorized access to personal information by a member or volunteer.
- Loss or theft of devices or documents containing sensitive information.
- Accidental disclosure of personal information to unintended recipients.
- Malicious cyberattacks or hacking attempts targeting NNSE systems or databases.

Detecting and Reporting: Any individual who suspects or becomes aware of a potential data breach must report it immediately to NNSE leadership.

Reports of data breaches should include detailed information about the incident, including the nature of the breach, the type of information compromised, and any actions taken or observed.

Response: Upon receiving a report of a data breach, NNSE leadership will conduct a prompt and thorough investigation to assess the scope and impact of the breach.

If the data breach poses a risk to the rights and freedoms of affected individuals, NNSE will

notify the relevant authorities and affected individuals without undue delay, as required by applicable data protection laws.

NNSE will take immediate step to mitigate the impact of the data breach, including implementing additional security measures, providing support to affected individuals, and cooperating with authorities as necessary.

Documentation and Review: NNSE will maintain records of all data breaches, including details of the incident, response actions taken, and any remedial measures implemented. These records will be reviewed periodically to identify trends, improve incident response procedures, and prevent future breaches.

Training and awareness: NNSE will provide training and awareness-raising activities to all members and volunteers on data protection best practices. Including procedure's for detecting and responding to data breaches.

NNSE is committed to safeguarding the personal and sensitive information entrusted to us by our members and volunteers. By adhering to the Data Breach Policy and implementing robust security measures, we strive to maintain the trust and confidence of our community while fulfilling our mission to promote social enterprise and sustainable business practices.