

Data Protection Policy

This policy applies to:

- The UK office of Security 3000 Nationwide Ltd.
- Its branches and regions.
- All sessional workers operating on behalf of Security 3000 Nationwide Ltd.

It applies to all staff.

This policy is operational from: 20/09/2011

This Policy is due to be reviewed on or before: 20/09/2012

The purpose of this policy is to enable Security 3000 Nationwide Ltd to:

- Comply with the law in respect of the data it holds about individuals;
- Follow good practice;
- Protect Security 3000 Nationwide Ltd supporters, staff and other individuals
- Protect the organisation from the consequences of a breach of its responsibilities.

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

Security 3000 Nationwide Ltd will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

Security 3000 Nationwide Ltd recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- Keeping information securely in the right hands, and
- Holding good quality information.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Security 3000 Nationwide Ltd will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Security 3000 Nationwide Ltd has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately) — especially at branch level.
- Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access - especially at branch level.
- Failure to establish efficient systems of managing changes to branch volunteers, leading to personal data being not up to date.
- Harm to individuals if personal data is not up to date

- Insufficient clarity about the way sessional workers' or volunteers' personal data is being used e.g. given out to general public.
- Failure to offer choices about use of contact details for staff, volunteers, sessional workers or branch officers

The Data Protection Officer is currently Lloyd Winters, with the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

Each Branch Committee is responsible their branch's compliance with this policy and supporting guidance.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.


Significant breaches of this policy will be handled under Security 3000 Nationwide Ltd disciplinary procedures

Access

Any subject access requests will be handled by the Data Protection Officer
Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

All those making a subject access request will be asked to identify any branches or sessional workers who may also hold information about them, so that this data can be retrieved.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information. The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Signed:  Name : Lyn Hanna
Position: Managing Director Date : 27/09/2011