Data Security Policy

1. Introduction

The National Sprayer Testing Scheme (NSTS) needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet NSTS data protection standards and to comply with the law.

2. Why This Policy Exists

This data protection policy ensures that NSTS:

- Complies with data protection law and follows good practice
- Protects the rights of staff, members and suppliers
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of a data breach

3. Data Protection Law

The Data Protection Act 1998 describes how organisations, including NSTS, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

4. Policy Scope

This policy applies to:

- The head office of NSTS
- All staff and volunteers/consultants of NSTS
- All contractors, suppliers and other people working on behalf of NSTS.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

5. Data protection risks

This policy helps to protect NSTS from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, there could be damage suffered if hackers successfully gained access to sensitive data.

6. Responsibilities

Everyone who works for or with NSTS has some responsibility for ensuring data is collected, stored and handled appropriately. Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and these data protection principles.

However, these people have key areas of responsibility:

- The AEA Board is ultimately responsible for ensuring that NSTS meets its legal obligations.

- The AEA CEO is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered in this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data NSTS holds about them (also called ‘subject access requests’).
- Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
- The IT providers, currently Green City and Fusion Works, are responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data, for instance, cloud computing services.

7. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from the CEO.
- NSTS will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared.
- Personal data must never be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their manager if they are unsure about any aspect of data protection.

8. Personal Data Storage

These rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked office or filing cabinet.
- Employees should make sure paper printouts are not left where unauthorised people could see them, such as on a printer.
- Data printouts should be shredded or disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should only be stored directly to laptops or mobile devices when actual working access is required through such devices. Personal data should never be stored directly onto laptops.
- All servers and computers containing data should be protected by approved security software and a firewall.

9. Personal Data Use

Personal data is of no value to NSTS unless the organisation can make use of it. It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended and should be password protected.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

10. Data Accuracy

The law requires NSTS to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort NSTS should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated, for instance, by confirming a customer's details when they call.
- NSTS will make it easy for data subjects to update the information NSTS holds about them, for instance, via the company website.
- Data should be updated as soon as inaccuracies are discovered, for instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

11. Subject access requests

All individuals who are the subject of personal data held by NSTS are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligation.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by letter, addressed to the CEO at Samuelson House, 62 Forder Way, Peterborough, PE7 8JB. The data protection officer can supply a standard request form, although individuals do not have to use this.

The CEO will always verify the identity of anyone making a subject access request before handing over any information.

12. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, NSTS will disclose requested data. However, the CEO will ensure the request is legitimate, seeking assistance from the Board and from the company's legal advisers where necessary.

13. Providing information

NSTS aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

14. Other Relevant Information and Policy

- Privacy Policy
- Data Security Breach Policy
- Password Policy
- Computer Security Policy