Data Security Policy NSP Resources (and all trading names)

Email security

- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- Use spam filters on the computers or use an email provider that offers this service.
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender

IT security

- Install a firewall and virus-checking on all computers.
- Make sure that the operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow staff access to the information they need to do their job and don't let them share passwords.
- Password protect any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Install an anti-spyware tool.
- Be wary of fake websites and phishing emails. Don't click on links in emails or social media. Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website.
- Use social media, including personal blogs, in a professional and responsible way, without violating company policies or disclosing confidential information.

To protect our data, systems, users and customers we use the following systems:
Laptop and desktop anti-malware - AVG Internet Security/ Resolv Client/Super AntiSpyware
Desktop firewall - Windows 10

Staff training and security

All officers will undertake data protection training as relevant to their job role:

- so they know what is expected of them;
- to be wary of people who may try to trick them into giving out personal details;
- so that they can be prosecuted if they deliberately give out personal details without permission;
- to use a password
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);

- not to open spam – not even to unsubscribe or ask for no more mailings.
- Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee, client or company confidential information. Fraudsters and hackers can be extremely persuasive and manipulative.

Other security measures

- Check the physical security of the premises and ensure it is properly locked when vacant or overnight
- Take particular care of your computer and mobile devices when you are away from home or out of the office.
- Where confidential information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and shredded when no longer required.