Cyber Security and Data Protection Guidelines

With the onset of GDPR here are some simple guidelines we can all follow to keep the data we hold safe. A large proportion of data breaches occur because of lapses in cyber security

Good Practice

One of the best things any of us can do when handling personal data is think ethically. How would we feel about our data being used in the same situation? Would we be happy for our information to be shared or left lying around?

Here are some practical and procedural guidelines to help.

- Who has access to your computer? If others have access, password protect your user identity and your NGS files so that you know that you only have access. Always logout of your user identity
- Consider updating passwords regularly and making them stronger.
- Do not have shared logins for any software, apps etc? Always have a separate login for each user and always use your own login details, never somebody else's. Do not give your login details to others to use.
- Any documents containing personal data should be password protected. To do this click File and then Protect Document/workbook in any Microsoft Office software. You can also restrict how a document can be edited there.
- If you are sending personal data via email password protect the document and send the password separately.
- When sending emails to groups of people use the blind carbon copy (bcc) function for all recipients email addresses.
- Ensure anti-virus software and current operating systems are up to date on your computer and devices.
- Any paper documents that contain personal data should be stored appropriately and in a locked file when unattended. Take care if files are taken out to meetings or events as losing paper files constitutes a data breach.
- Ensure that any paper documents with personal details on that need to be destroyed are shredded.
- Do not leave any documents in printer trays that others have access to, that contain personal data for too long.
- If you get asked for garden owner's details (this includes photos) by outside organisations, consider the following before giving them out.
- *Have they explicitly consented to this in advance?*
- *If no, contact them first and make a note in your records, as to the permission given.*

Do we need this data?

Under GDPR, when storing any personal data we need to make sure we are only storing what we need and not info just in case.

- We need to make sure that data is kept up to date and refreshed regularly. Requests to update data should be processed in a timely fashion.
- We should not store data for longer than we need to.

- We should ensure data is accurate and up to date but we shouldn't just fill in gaps without the data subject's permission.
- We also have to respect any individuals request to have their personal data removed from our systems. Please speak to your Data Manager as to the correct procedure for this.
- We also have to be prepared to share any data we hold on them at their request within a timely fashion (within 30 days). Therefore we must make sure that any notes we hold on a data subject (individual) we are happy for them to see.

Emails

Many data breaches occur because of malicious emails and it is becoming increasingly difficult to spot these. Here are some ways to check whether an email is genuine or not.

- Hover over the email sender's name to see if it is actually from them (e.g. emails can show up as coming from a company like Amazon, but when you scroll over the Amazon name you will see the email address is made up of random characters or from a dodgy email address. Always scroll over the name to check, don't click!
- Even if you scroll over the email address and it looks genuine beware that scammers are getting more sophisticated and can make email addresses look very genuine, or could even have hacked into someone's account. Always double check if an email asks you to send money or sensitive information, even if the sender appears genuine.
- Do not click on any links in an email that you are not sure of. Again scroll your mouse (don't click) over the link to see what it actually is.
- Many malicious emails are badly written with spelling mistakes and bad grammar, although they are getting better at this.
- Many malicious emails will have sensational titles designed to get you to panic that it is urgent and get you clicking. Always stop and follow the above steps to check if it is genuine.
- Similarly if something seems too good to be true, i.e. you've won a lottery you never entered, it probably is.
- If you get an email asking you to login to an account, don't click on the link but go online and login via the website you would normally login from.
- If you get an email from someone internally asking you to do something out of the ordinary (ie transfer a large amount of money), give them a call and double check the email originates from them.
- Finally avoid emails from Nigerian Princes or people on holiday requesting money, like the plague!
- If in doubt always check with the Data Protection Manager or Deputies at head office.

If you feel you have received a scam email

- Forward to head office, do not reply.
- Block the sender and check that their email address hasn't been remembered in your system as a contact for who they are pretending to be.
- Change your password
- If you have replied to the email or sent any details of our organisation to a scammer, or if you feel they may have gained access to your computer please refer to our document What to do if you suffer a data breach and **contact Head Office immediately**.

We advise that all members of County Teams use an ngs.org.uk for NGS business as we can protect you better from scams that way. If you do not have an ngs.org.uk email address please let head

office know. However we cannot totally prevent scam emails, so awareness and double checking is key to stopping any potential breaches.

New Projects

For any new project we undertake that will collect personal data we need to complete a DPIA (Data Protection Impact Assessment) which will include what the data collection process will be, why we are collecting the data etc. We will have a form for this which the Data Protection Manager will complete, with input from relevant staff. These will need to be completed before any new project begins so please speak to Jo McGowan before any data collection commences.

We will need to do this for every data collection process we have currently too.

Any questions, doubts or help needed just speak to Jo – joanne@ngs.org.uk or 01483 213905.

Data Protection Manager – Jo McGowan, joanne@ngs.org.uk, 01483 213905

Deputy Data Protection Manager – Georgina Waters – georgina@ngs.org.uk, 01483 211795

Deputy Data Protection Manager – George Plumptre – george@ngs.org.uk, 01483 213906