LICKEY AND BLACKWELL PARISH COUNCIL

Data Breach Procedure

Lickey and Blackwell PC understand that a personal data breach isn't only about loss or theft of personal data.

Personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

We have a response plan for addressing any personal data breaches that occur. Our Executive Officer has the responsibility for managing breaches.

Responding to a personal data breach

All Council members are at risk of a personal data breach and should take precautions to prevent those. To protect yourself from risk follow the advice given in the Security Advice appendix below.

If you suspect that you have been subject to a data breach, contact the Executive officer eo@lickeyandblackwellpc.org/ 07930837770 as soon as possible.

The EO will notify the ICO of a breach within 72 hours of becoming aware of it. The EO will inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms without undue delay. The EO documents all breaches, even if they don't all need to be reported.

APPENDIX – SECURITY ADVICE

PLEASE NOT COUNCILLORS SHOULD NOT STORE CONFIDENTIAL PARISH MATERIAL AT HOME

Computer security

Install a firewall and virus-checking on your computers.

Make sure that your operating system is set up to receive automatic updates.

Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.

Do not share passwords.

Encrypt 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).

Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Email security

When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". 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. WE SHOULD ALWAYS BCC WHEN WE EMAIL A GROUP OF RESIDENTS.

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.

If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Other security measures

Shred all your confidential paper waste.

Check the physical security of your premises.

Be wary of people who may try to trick them into giving out personal details;

Use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;

Do 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);

Do not open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

Approved by the Parish Council on 22nd May 2023

Review date May 2024