Ludgvan Parish Council

Council IT, internet and email policy

Introduction

The purpose of this policy is to ensure that all employees and any volunteers or Members using Ludgvan Parish Council IT have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the council's equipment, safeguard the security of its IT systems and data, and assist compliance with Data Protection law.

The policy should be read in conjunction with our Communications Policy and Data Protection Policy.

Policy coverage

This policy covers the security and use of all the council's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment.

ACCEPTABLE USAGE

Computer access

Access to the council's IT systems is controlled by the use of user ID's and passwords. Individuals must not:

- Leave their user accounts logged in at an unattended and unlocked computer
- Leave their password unprotected
- Perform any unauthorized changes to the IT systems or information
- Attempt to access data that they are not authorized to use or access
- Connect any unauthorized device to the council's network or IT systems
- Store council data on unauthorized equipment
- Give or transfer council data or software to any person or organization outside the council without the appropriate authority to do so

Individuals must not store personal files, such as music, video, photographs or games, on council IT equipment.

Internet and email conditions of use

The council's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the council in any way, not in breach of any terms and conditions of employment and does not place the individual or the council in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Internet access unacceptable behaviour

In particular, the following is deemed unacceptable use or behaviour

- Visiting sites that contain obscene, hateful, pornographic or illegal material
- Perpetrating any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users

- Downloading commercial software or any copyrighted materials belonging to third parties, unless the download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorized system, sites or files
- Publishing defamatory and/or knowingly false information about the council, colleagues, Members and/or customers on social networking sites, blogs, wikis or any online publishing format
- Revealing confidential information about the council in a personal online posting, upload or transmission; including financial information and information relating to employees, Members and/or internal discussions
- Introducing any form of malicious software into the council network

Email usage unacceptable behaviour

In particular, the following is deemed unacceptable use or behaviour:

- Distributing, disseminating or storing images, text or materials that are illegal, or might be considered indecent, pornographic or obscene
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered harassment
- Use of council communications systems to set up personal businesses or send chain letters • Forwarding council confidential messages to external locations
- Accessing copyright information in a way that violates the copyright
- Broadcasting unsolicited personal views on social, political, religious or other non-council related matters or transmitting unsolicited commercial or advertising material

Emails should not be kept longer than they are required in line with our Data Protection Policy.

Users should be aware of the characteristics of spam and phishing emails and should not reply to these emails, but add the sender to the email system's blocked senders list.

Actions upon termination of contract of employment, or cessation of term of office of councillors

All council equipment and data, for example laptops and mobile devices, must be returned to the council when employees/councillors leave the council.

Monitoring and filtering

All data that is created and stored on council computers is the property of the council and there is no official provision for individual data privacy. However, wherever possible the council will avoid opening personal emails.

The council maintains the right to examine any systems and inspect any data recorded in those systems, which includes but is not limited to internet access and email or messaging content. As a matter of compliance with this policy and meeting the regulatory requirements asked of the council, the council reserves the right to use monitoring software in order to check upon the use and content of emails. The council maintains the right to monitor the volume of internet and network traffic, together with internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Any monitoring will be carried out in accordance with audited, controlled internal processes, current UK Data Protection law, the Regulation of Investigatory Powers Act 2000 and the elecommunications

(Lawful Business Practice Interception of Communications) Regulations 2000. Any individuals who suspect a breach of security policy must report it without delay to the Parish Clerk. All breaches of information security policy will be investigated and where investigations reveal misconduct, disciplinary action may follow in line with the council's Disciplinary Policy and Procedures. Breaches of the IT Policy by Members could contravene the Code of Conduct and action may result from this contravention.

Reporting loss or theft

In the event of loss or theft of any mobile device, irrespective of whether it is council-issued or personally owned, the user must act promptly to minimise the risk of compromise to council information by immediately:

- Reporting theft of device to the police
- Reporting the loss or theft to the clerk / parish council chairman as appropriate
- Changing any passwords that may have been used on the device, eg banking

Adopted:

Due for review: