Clerk: Mrs Sarah Rimell
Illogan Parish Council Community Office, Trevelyan Road, Illogan, TR16 4RG
Telephone: 01209 711433
Email: enquiries@illoganparishcouncil.gov.uk

Use of IT Policy

Introduction

The Use of IT Policy is designed to protect Illogan Parish Council and its employees from harm caused by misuse of our IT systems and data. Misuse includes both deliberate and inadvertent actions.

The consequences of the misuse of IT systems can be severe. Examples of potential damage include, but is not limited to, malware infections, legal and financial penalties for data leakage and lost productivity resulting from network downtime.

Everyone employed by Illogan Parish Council is responsible for the security of the IT systems and the data on them. As such, all employees must ensure that they adhere to the guidelines in this policy at all times. If employees are unclear on the policy or how it impacts their role they should speak to their line manager.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Illogan Parish Council. These rules are in place to protect the employee and Illogan Parish Council.

To enable employees to complete their jobs effectively Illogan Parish Council provides its employees with access to appropriate forms of electronic equipment, media and services, including computers, email, telephone, voicemail, internet and the world wide web.

Illogan Parish Council encourages the use of media and associated services because they can make communication more efficient and effective and because they are valuable sources of information. However, all employees and everyone connected with the Council should remember that electronic media and services provided are the property of the Council and their purpose is to facilitate and support Council business. All computer users have the responsibility to use these resources in a professional, ethical and lawful manner.

Definitions

"Users" are everyone who has access to any of Illogan Parish Council's IT systems. This includes permanent employees, temporary employees, contractors, agencies, consultants and suppliers.

"Systems" means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, phones, tablets, printers, data and voice networks, networked devices, software, electronically stored data, portable data storage devices, third party networking services and all other similar items commonly understood to be covered by this term.

Adopted: 28.01.15 Minute Number: FR15/01/17.2

Clerk: Mrs Sarah Rimell
Illogan Parish Council Community Office, Trevelyan Road, Illogan, TR16 4RG
Telephone: 01209 711433
Email: enquiries@illoganparishcouncil.gov.uk

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Illogan Parish Council's business. All employees, contractors, consultants, temporary, and other workers at Illogan Parish Council are responsible for exercising good judgement regarding appropriate use of information, electronic devices and network resources in accordance with Council policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Illogan Parish Council. This policy applies to all equipment that is owned or leased by Illogan Parish Council.

Use of IT Systems

All data stored on Illogan Parish Council's systems is the property of Illogan Parish Council.

Illogan Parish Council's systems exist to support and enable the business of the Council. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleagues productivity, the security of the IT systems and nor should it result in any direct costs being borne by Illogan Parish Council other than for trivial amounts (e.g. an occasional short telephone call).

Illogan Parish Council trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the Council's IT systems.

Any information that is particularly sensitive or vulnerable must be encrypted in transit and at rest so that unauthorised access is prevented (or at least made extremely difficult). However this must be done in a way that does not prevent-or risk preventing-legitimate access by all properly-authorised parties.

Illogan Parish Council can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history by any users.

For security and network maintenance purposes, Illogan Parish Council or authorised individuals may monitor equipment, systems and network traffic to ensure compliance with this policy. Illogan Parish Council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Employees have a responsibility to promptly report the theft, loss or unauthorised disclosure of Illogan Parish Council's proprietary information.

You may access, use or share Illogan Parish Council's proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

Adopted: 28.01.15 Minute Number: FR15/01/17.2

Clerk: Mrs Sarah Rimell
Illogan Parish Council Community Office, Trevelyan Road, Illogan, TR16 4RG
Telephone: 01209 711433
Email: enquiries@illoganparishcouncil.gov.uk

Data Security

If data on Illogan Parish Council's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-council system any information that is designated as confidential, or that they should reasonably regard as being confidential to Illogan Parish Council, except where explicitly authorised to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts.

Users who are supplied with computer equipment by Illogan Parish Council are responsible for the safety and care of that equipment, and the security of software and data stored on it and on other Illogan Parish Council systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be taken with these devices: sensitive information should be encrypted in transit and at rest. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) must be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g. viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported to Illogan Parish Council's systems by whatever means and must report any actual or suspected malware infection immediately.

Unacceptable Use

The following activities are, in general, prohibited. All employees should also use their own judgement regarding what is acceptable use of Illogan Parish Council's systems. The activities below are examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or

services. These also include activities that contravene Data Protection Regulations and activities that contravenes the Computer Misuse Act 1990.

- All activities detrimental to the success of Illogan Parish Council. These include sharing sensitive information outside the Council.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the Council. These include activities that slow down the computer network (e.g. streaming music or video, playing networked video games).

- All activities that are inappropriate for Illogan Parish Council to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.

- Circumventing the IT security systems and protocols that Illogan Parish Council has put in place.

Enforcement

Illogan Parish Council will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgement regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.

Use of Illogan Parish Council's resources for any illegal activity will be classed as gross misconduct and could result in instant dismissal. Illogan Parish Council will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Review Date	Reviewed By	Amendments	Minute Number
08.02.17	Governance Review Committee	None	GR17/02/26.2
13.06.18	Governance Review Committee	Typo on page 1 corrected 'more' not 'for'	GR18/06/20.2
27.02.19	Governance Review Committee	None	GR19/02/36.2
23.03.22	Governance Review Committee	• Page 4 – Unacceptable Use – 2nd bullet point – 2nd sentence – amend to read 'These include sharing sensitive information outside the Council.'	GR22/03/21.2
27.09.23	Governance Review Committee	• Page 2 – Use of IT Systems – 4th paragraph – amend to read 'Any information that is particularly sensitive or vulnerable must be encrypted in	GR23/09/21.2

Clerk: Mrs Sarah Rimell
Illogan Parish Council Community Office, Trevelyan Road, Illogan, TR16 4RG
Telephone: 01209 711433
Email: enquiries@illoganparishcouncil.gov.uk

		transit and at rest so …' • Page 3 – Data Security – 6th paragraph – amend to read 'Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be taken with these devices: sensitive information should be encrypted in transit and at rest.'	
27.03.24	Governance Review Committee	None	GR24/03/20.2