IT Policy V1.0 – Westleton Parish Council

Information Technology Acceptable Use, e-Safety and Social Media Policy, Procedure and Guidelines

1. Purpose

Insecure practices and malicious acts expose Westleton Parish Council (thereafter referred to as WPC) and individuals using its systems to risks including virus attacks, compromise of network systems and services, and loss of data or confidential information. In addition, security breaches may damage WPC's reputation and could result in loss of services. Other misuses, such as excessive use by an individual, can substantially diminish resources available for other users. This purpose of this Policy and Procedure is to provide information on what is expected of individuals using WPC's Information Technology (IT) systems and what is deemed as acceptable use of those systems.

Digital Media platforms (such as a website) open up many new and exciting opportunities, however, the practical application of such technology by WPC is continually developing. To avoid circumstances which could result in reputational, legal and ethical issues, and misuse/abuse of a well-functioning digital media relationship, it is important that WPC manages any potential risks through a common-sense approach and framework as well as proactively monitoring the development of such applications.

2. Definitions

This Policy and Procedure applies to all WPC councillors, employees, agency workers, volunteers and trustees, collectively referred to as 'staff' in this document.

This Policy and Procedure applies to all IT resources owned or leased by WPC and to any privately owned equipment connected to the network and includes, but is not limited to, computer equipment, mobile devices, software, operating systems, storage media, the network, and the internet.

Digital media is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online and includes online social forums, blogs, video- and image-sharing websites and similar facilities.

3. Policy

WPC is committed to protecting itself from unethical, illegal, or damaging actions by individuals using its IT resources and aims to ensure that WPC staff have access to reliable and robust IT resources that are safe from unauthorised or malicious use.

Unless otherwise specified, the use of WPC IT resources is restricted to purposes related to WPC's operational activities. Authorised staff are provided with access to appropriate resources in order to support them carrying out their work- related activities. Staff may not share with, or transfer to, others any information relating to their WPC IT accounts including network IDs, passwords, or other access codes that allow them to gain access to WPC's IT resources.

WPC is committed to making the best use of all available technology and innovation to improve the way we do business. This includes using all reasonable and cost-effective means to improve the way we communicate, reach out and interact with the different communities we serve through the use of social media. Staff must follow the approved procedures concerning the use of, or the development of, any social media application, and to help them get the best out of the tools available whilst maintaining a safe professional environment and protecting themselves, as well as WPC.

Procedure and Guidelines

1. Acceptable Use and e-Safety Definition

The phrase "e-Safety" in this procedure defines general advice and what is classed as "acceptable" use of a range of WPC IT Resources such as computer systems, networks, devices, email and much more. Individuals are prohibited from engaging in any activity that is illegal under UK laws. The advice below is not exhaustive but attempts to provide a framework for activities that fall into the category of unacceptable use and also gives related general advice.

2. Email

2.1 Information

Each staff member will be issued with a specific .gov email address from the approved IOMart domain system used by WPC.

E-mail is not a confidential means of communication. Staff should bear in mind that e-mail messages can be very easily read by those for whom they were not intended and in particular recognise that e-mails can be:

- intercepted by third parties (legally or otherwise)
- wrongly addressed
- forwarded accidentally
- forwarded by initial recipients to third parties against your wishes
- viewed accidentally by others on recipients' computer screens

Sensitive personal data should not be communicated by e-mail unless the express permission of the subject has been obtained or unless adequate encryption facilities have been employed.

When opening external e-mails, individuals should be aware that attachments may contain viruses and be very careful if there is any suspicion of it including a virus. If a member of staff has any suspicions, they must not open the attachment and should contact the IT team immediately.

Remote access to WPC email services is permitted via the IOMart webmail service available across multiple types of web browsers. Loading of the WPC email service onto a device-specific client is not approved.

Logging and backup of email mailboxes for all staff occurs on an on-going daily basis and is stored for at least 1 month, in line with its supplier backup procedures. WPC, via authorised staff, reserves the right to inspect these logs and backups at any time for any reason.

Staff are provided with 50GB of email storage and are expected to keep within this limit.

Staff are prohibited from using any e-mail account that is not provided by WPC for its business. In this case each councillor will be issued with a specific .gov email address for exclusive WPC use.

2.2 The WPC email system may not be used by staff for inappropriate reasons which include:

- Sending unsolicited messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material.
- Engaging in harassment via electronic communications whether through language, frequency, or size of messages.
- Masquerading as someone else by using their email address or email signature.
- Creating or forwarding "chain letters" or solicitations for business schemes.
- Sending emails for non-CAD related commercial use or for personal gain.
- Sending deliberately false, defamatory or malicious information to WPC contacts, stakeholders and partners regarding WPC, its staff, board members, suppliers, partners and stakeholders.
- Creating or transmitting of any offensive, obscene or indecent images, data or other material.
- Transmitting material which infringes the copyright of another person, including intellectual property rights.

3. System and Network

3.1 Information

- Staff are responsible for the security of data, accounts, and systems under their control. Passwords must be kept secure and account or password information

must not be shared with anyone, including other staff, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

- Staff who have been provided with mobile devices such as mobile phones, tablets, laptops etc. are responsible for ensuring these devices are securely stored when not in use.
- All data stored on WPC's systems is the property of WPC.
- WPC can monitor the use of its IT systems and the data on it at any time. This may include examination of the content stored within the email and data files of any user, and examination of the access history of any users. WPC reserves the right to regularly audit networks and systems to ensure compliance with this policy and procedure.

3.2 Personal Use of Resources

- Undertaking WPC business on personal devices should only be using web-access with no local resident client storing offline data. Undertaking non-WPC work on WPC IT resources (if provided) is not allowed.
- WPC's systems exist to support and enable the parish council business, and should not be used for personal purposes.

3.3 The system and network activities are may not be used by staff for inappropriate reasons which include:

- Engaging in or effecting security breaches or malicious use of network communication including, but not limited to:
    - Obtaining configuration information about a network or system for which the user does not have responsibility.
    - Engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully create nuisance traffic for the network or systems attached to the network.
    - Accessing data, accounts, or systems that the user is not expressly authorised to access.
    - Interfering with or denying service to another user on the network or using WPC facilities or networks to interfere with or deny service to persons outside WPC.
- Use of file sharing networks in which protected intellectual property is illegally shared.
- Intentionally introducing malicious programs into the network or server e.g., viruses, worms, Trojan horses, email bombs, etc.
- Inappropriate use or sharing of WPC-authorised IT privileges or resources.
- Changing another user's password, access, or authorisations, unless expressly authorised to.

- Using a WPC IT asset for any private purpose, or for personal gain.
- Using a WPC IT asset to access pornographic material.

3.4 Password Security

Secure and strong passwords are essential to protect the integrity of ICT systems. Staff will be issued with a username & password for each email account. No changes can be made without express permission of the Parish Clerk.

- Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.
- You must only use your own login and password when logging into IOMart systems.
- Where temporary passwords are issued to any individual, for any reason, then they should be changed at first logon to a permanent password, subject to agreement with the Parish Clerk.

3.5 Viruses

Viruses can expose WPC to very considerable risks. You are required to take all reasonable steps to avoid the introduction of any virus on WPC equipment, systems or networks. Reasonable steps will include, but are not limited to:

- not using any removable media, such as a memory stick, unless encrypted and with prior approval from the Parish Clerk.
- be cautious when opening any emails that you are not expecting especially those that contain an attachment.
- do not follow any links to questionnaires, offers, requests, etc. from unknown sources - delete the email.
- delete emails with attachments that you were not expecting even if you know the person sending, if the wording seems “odd” in some way. These programs can often spoof the Sender field in emails to make it look like someone you know is emailing you.
- not installing any hardware or software without the express permission of the parish Clerk.
- allowing any anti-virus software installed on WPC equipment to run as it needs to and not interrupting or in any way interfering with such software.
- If you suspect there may be a virus on any WPC equipment, you must stop using the equipment and contact the Parish Clerk immediately for further advice.
- Reporting a suspected phishing email if you receive one to the Parish Clerk so that it can be safely checked, and further guidance issued.

4. Internet

4.1 Information

WPC staff are expected to proceed with caution when accessing the internet on WPC devices. Whilst security and anti-virus software is installed on all laptops and desktops, staff are expected to be particularly aware when viewing sites that they have not visited previously and/or if pop up boxes are displayed on the website and in these circumstances, particular caution should be exercised.

4.2 The internet may not be used by staff for inappropriate reasons which include:

- Downloading any software from the internet without prior approval of the IT team.
- Downloading copyrighted material such as music media (MP3) files, film and video files, note that this in (not an exhaustive list.
- Connecting WPC devices to the internet using non-standard connections or connection types that have not been agreed with the IT team.
- Using the internet from WPC devices or premises to gamble.
- Placing or altering any information on the internet that relates to WPC or expressing any opinion about WPC unless they are specifically authorised to do so.
- Using the internet from WPC devices or location for reasons detailed in paragraph 3.3.

5. Intellectual Property/Copyright

5.1 Information

Staff may not use WPC facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property

5.2 Intellectual Property violations which staff must not undertake include:

- Engaging in unauthorised copying, distribution, display, or publication of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.
- Using, displaying, or publishing licensed trademarks, including WPC's trademarks, without license or authorisation or using them in a manner inconsistent with the terms of authorisation.
- Using or displaying images of individual unless permission has been agreed in accordance with the Media Policy.

6. Social Media

6.1 Information

WPC encourages staff, who are authorised to do so, to make reasonable and appropriate use of social media as part of their work as it is recognised that it is an important part of how WPC communicates. Staff will be authorised to use social media by the Parish Clerk.

Staff must be aware at all times that, whilst contributing to WPC's social media activities, they are representing WPC.

Staff who use social media as part of their job must adhere to the same safeguards as they would with any other form of public communication about WPC in the public sphere. These safeguards include:

- ensuring that the communication has a purpose and a benefit for WPC;
- obtaining permission from the Parish Clerk before embarking on a public campaign using social media; and
- getting a colleague to check the content before it is published.

6.2 Social media used by staff must not:

- breach confidentiality, for example by:
    - revealing confidential intellectual property or information owned by WPC or;
    - giving away confidential information about an individual or WPC; or discussing WPC's internal workings, such as agreements that it is reaching with partners/customers or its future business plans that have not been communicated to the public,
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age or;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content or;
- bring WPC into disrepute, for example by:
    - criticising or arguing with students, customers, colleagues, partners or competitors or;
    - making defamatory comments about individuals or other WPCs or groups; or
    - posting images that are inappropriate or links to inappropriate content or;
- breach copyright, for example by:

- using someone else's images or written content without permission; or
- failing to give acknowledgement where permission has been given to reproduce something.

6.3 Personal use of social media

WPC recognises that many staff make use of social media in a personal capacity. While they are not acting on behalf of WPC, employees must be aware that they can damage WPC if they are recognised as being one of our employees.

Staff are allowed to say that they work/volunteer for WPC, and it is recognised that it is natural for staff to want to discuss their work on social media. A staff member's online profile, for example, the name of a blog or a Twitter name, must not contain WPC's name.

If staff discuss their work on social media, for example, giving opinions on their specialism or the voluntary and community sector, they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer."

Any communications that staff make in a personal capacity through social media must not breach the criteria given in paragraph 6.2.

7. Video Conferencing (via Teams, Zoom etc)

7.1 Information

As part of most job roles within WPC, it may be a necessary requirement to use video conferencing facilities such as Microsoft Teams, Zoom or others to consult with other internal staff or external partners or stakeholders. These platforms may also be used to produce online training, webinars and workshops by agreement with a Senior Manager and are also covered by this policy.

Staff who use types of online platform as part of their job must adhere to a variety of safeguards to ensure that WPC's reputation and standing is not affected. All WPC staff can use video conferencing facilities for online meetings with partners and other staff but specific guidelines and safeguards include:

- Invites to video conferencing sessions hosted by WPC staff should only be sent to those people strictly required/booked for the session. These details should not be shared with anyone else.
- Treat any video conferencing meeting or session like a physical conversation. Only discuss items that are required as part of your discussion – Remember that the other person could be recording the session without your knowledge.

- Ensure that you enable a “lobby”/waiting room feature so that only authorised users can access the meeting or session unless there is a very specific reason not to do so. Normally these features should be enabled by default but it is the host (staff member) responsibility to check.
- If you are the host, end the session in the appropriate manner (dependent on the chosen application) to ensure it closes any ability for people without the correct authentication can get into the video conferencing session.
- Ensure that any confidential physical information in your room or office setting is not in public view of your camera.
- Ensure that your microphone does not pick up confidential or inconsequential discussions elsewhere in your environment, use headphones where possible.
- In instances where video conferencing is conducted directly from users’ desks, cameras should be positioned to focus solely on the individual, and the sensitivity of the microphone should be tuned to a minimum to reduce the risk of other conference participants seeing or hearing something inappropriate.
- The latest video conferencing applications boast features such as file exchange, remote camera control and screen sharing and these should be disabled unless they are required. Remote control of cameras should only be allowed by authenticated and trusted users. Consider this also when dealing with third parties who may be collaborating with you on one project but are competitors in others.

8. Working from home or out of the office

8.1 Information

You may be supplied with WPC equipment to utilise at home and outside of your usual workplace setting. This includes laptops, tablets, mobile phones and mobile storage devices. Such equipment must be treated and used in the same way as it would be in the workplace. You are expected to abide by this policy when using all such WPC equipment. You should abide by all the following points when working from remotely or out of the office.

- Users should be aware of the physical security dangers and risk associated with working within any remote office or mobile working location.
- Family members are not allowed to use any WPC provided ICT devices.
- When not in use, all WPC Devices should be switched off, logged off, or the keyboard locked.
- Data must be saved to the WPC network via the approved network storage space. Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is absolutely necessary to do so, then this should be for as short a period as possible, and the local drive must be encrypted.
- You are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.

- On termination of employment, resignation or transfer, you must return all equipment to a member of the Parish Council. You must also provide details of all of your system logons so that they can be disabled.
- Equipment provided by WPC must never be left unattended in an area accessed by the public and/or when travelling. When travelling by car, if you have to leave the car unattended then equipment should be kept locked in the boot and out of sight where it is not possible for you to take the equipment with you. Connections to “public” or other WPC’s Wi-Fi access points is allowed but a set of guidance is shown below.
    - If connecting to a public wifi access point then be aware of your surroundings. If someone is acting suspiciously around, you (within 20 metres) then disconnect from the wifi network immediately and close your laptop
    - If connected to a public wifi access point, browse websites that only have the “secure” lock symbol which indicates that site data is being encrypted.

Inappropriate use or failure to follow these standards may result in removal of staff access to WPC equipment & Digital Services.

I have read the document & understand the terms of use for Digital Services as it relates to Parish Council business.

Name……

Signature……

Date……