# SOUTH WAIRARAPA DISTRICT COUNCIL

**9 AUGUST 2017**

---

**AGENDA ITEM C3**

# INFORMATION AND TECHNOLOGY POLICY N600 REVIEW REPORT

---

## Purpose of Report

To inform Councillors of the proposed changes to the Information and Technology (IT) Policy N600.

## Recommendations

Officers recommend that the Council:

1. *Receive the information.*
2. *Approve the amendments to the Information and Technology (IT) Policy N600.*
3. *Agree the next review date should be June 2020.*

## 1. Executive Summary

The Information and Technology Policy N600 was due for review in June 2017. The amended policy has been drafted and needs approval by Council.

## 2. Background

Information and technology (IT) is a key part of any business operation and is provided to support the organisation's core business. IT systems should improve the operational efficiency and productivity of all staff.

Officers have reviewed the IT policy and recommend a number of changes.

## 3. Summary

The revised policy provides direction for the responsible use of Email, Internet and telecommunications services by Council staff.

The policy also covers:

- Prohibited activities while using SWDC IT services e.g. downloading objectionable material, online gambling
- Management of the SWDC website

- Appropriate use of telephones, mobile phones, e-mails and facsimiles
- Recommended practices for retention of e-mails
- Appropriate use of information downloaded from the internet
- The need to abide by all software licensing agreements, copyright laws and other applicable regulations.
- A new clause has been added covering the use of social media (Clause 4.8).

As the new policy has significant changes from the current IT policy, tracked changes have not been used in the attached document.

## 4. Conclusion

The revised IT policy has been reviewed by the senior management team, the IT contractor and the Audit and Risk working party.

It is now submitted to Council for their review and approval before circulating to staff for implementation.

## 5. Appendices

Appendix 1 - Information and Technology (IT) Policy N600

Contact Officer: Jennie Mitchell, Group Manager Corporate Support
Reviewed By: Paul Crimp, Chief Executive Officer

# Appendix 1 – Information and Technology (IT) Policy N600

# INFORMATION AND TECHNOLOGY POLICY

## 1 Introduction

This policy sets out guidelines for South Wairarapa District Council (SWDC) personnel regarding the use of information technology at SWDC.

## 2 Purpose of Information Technology

- Information and technology (IT) is provided to support the organisation's core business, to simplify how work is done and make it easier for people to access and use information
- IT systems should facilitate access to the wealth of information collected throughout the sector and provide flexibility for future organisational and technology changes.
- IT systems should improve the operational efficiency and productivity of all staff.

## 3 Purpose of this Policy

- To provide direction for the responsible use of Email, Internet and telecommunications services by Council staff.
- To protect Council from threats to its information system from viruses and unauthorised software.
- To protect users against unreasonable exposure to risk, objectionable material and allegations of impropriety.

## 4 Electronic Communications

Electronic communications (phone, mobile phone, photographic/video or Internet based) are council's property and part of the public record, and as such, must be retained or disposed of in accordance with the Archives New Zealand Electronic Record Policy and the SWDC Retention and Disposal Agreement, in accordance with the Public Records Act.

### 4.1 Legal status

Electronic communications may be used as evidence in a court of law. This includes deleted material and private mail obtained from system backups. (Electronic Transactions Act 2002).

### 4.2 Context

Electronic communication must be undertaken in a manner which contributes to the safe, effective and accountable operation of the SWDC.

The Electronic communication systems must be kept clear of unchecked and unnecessary mail.

### 4.3 Scope

These policies apply to all staff and to any other person authorised to have access to the SWDC information systems.

### 4.4 Appropriate Use - Email

a. Staff may only use their own email address to send or receive emails.

b. Use of the email and Internet is permitted and encouraged for business purposes which support the goals and objectives of the SWDC.

c. The Email and Internet are to be used in a manner that is consistent with SWDC's normal standards of business conduct and communication and as part of the normal execution of an employee's responsibilities.

d. Examples of appropriate use include:

e. Email communication with colleagues within SWDC or in other Agencies or other business contacts.

f. Conducting research for SWDC projects.

g. Retrieving news stories or other information of general work related interest.

h. Staff may utilise the email facility for brief messages of a non-official nature, on an occasional basis. For this purpose, a file involving more than one normal page of text would be significant. Employees who choose to use this privilege do so in the knowledge of and consent to the SWDC's monitoring policy set out above.

i. Users should take all sensible measures to reduce the size of attachments being sent by email, pdf or zip or use hyperlinks when sending internal emails.

### 4.5 Personal Use - Internet

a. Staff may utilise the internet facilities for personal use, provided the data transmission involved is not of a significant nature. Employees who choose to use this privilege do so in the knowledge of and consent to the SWDC's monitoring policy set out above.

b. Your job comes first. Unless you are authorized to use social media as part of your role e.g. to update SWDC's facebook page, don't let social media affect your job performance.

c. Employees are not allowed to disclose SWDC financial, operational or legal information, or any information that pertains to ratepayers and other customers and should at all times abide by the requirements of their employment contract and code of conduct with regard to confidential information.

d. Dishonourable content such as racial, ethnic, sexual, religious, and physical disability slurs are not tolerated

e. Proper copyright and reference laws should be observed by employees when posting online.

f. Employees are allowed to associate themselves with SWDC when posting but they must clearly brand their online posts as personal and purely their own. SWDC should not be held liable for any repercussions the employee's content may generate.

### 4.6 Other Matters

a. Users must abide by all software licensing agreements, copyright laws and other applicable regulations.

b. Email is an insecure method of communication and must be treated with caution. Care should be taken to ensure that e-mail sent out is addressed correctly. It should be noted that E-mail does not provide any guarantee of delivery.

c. Users must only access internet from computers they are logged into using their own username.

d. Staff may not download any software onto SWDC Computers without approval from their Manager/Team Leader and the IT department.

### 4.7 Information Sourced from the Internet

a. The presence of information on the Internet does not mean that there is a right to copy. Information may only be copied where the author has expressed or implied authorised copying can occur.

b. Staff should not include any information protected by copyright in any Internet publication unless permission has been officially provided.

c. Users should be aware that information on the Internet may be inaccurate or untimely and there is a danger that opinions may be presented as facts. All information should be validated before using for business purposes.

### 4.8 Social Media including Facebook

a. SWDC staff participating online should participate in the same way as they would with other media or public forums such as speaking at conferences.

b. Staff should seek authorisation to participate in social media on behalf of SWDC. They should not disclose information, make commitments or engage in activities on behalf of SWDC unless they are authorised to do so.

c. Staff need to remember that participation online results in their comments being permanently available and open to being republished in other media.

d. Staff need to stay within the legal framework and be aware that defamation, copyright and privacy laws, among others, apply.

e. If using social media in a personal capacity, staff should not identify their employer when doing so would bring your employer into disrepute

f. Staff should keep in mind that even social media sites restricted to 'friends' are in effect public, as they cannot control what friends do with the information.

g. Staff should always make sure that they are clear as to whether they are participating in an official or a personal capacity. They need to be aware that participating online may attract media interest in them as an individual, so they need to proceed with care regardless of what capacity they are acting in.

## 5 Prohibited Activities

Staff may not use the Internet or email for inappropriate purposes. Examples of inappropriate use include:

- Storing, uploading or downloading software or electronic files for personal use other than as outlined in clauses 4.4 and 4.5.
- Accessing, transmitting, storing, uploading or downloading material which is obscene, objectionable or likely to be offensive.
- Gambling
- Conducting illegal activities
- Soliciting for personal gain or profit or conducting any personal commercial or commercially related activities
- Making or posting indecent remarks and proposals or conducting any form of harassment
- Uploading or downloading commercial software in violation of its copyright
- Downloading any software or electronic files without reasonable virus protection measures in place
- Passing off their own views as representing those of the SWDC.
- Playing and/or downloading games.
- Sending electronic "chain letters".

## 6 Responsibilities

The Information Technology (IT) Contractor is responsible for:

- Ensuring that the policy and guidelines governing Email and Internet access meet good information management practices and IT security requirements
- Ensuring the availability of support resources to handle Email and Internet user access/installation requirements
- Ensuring the continued availability of the LAN and connections between the LAN and the gateway through which the Internet is accessed

- The management of Email and Internet service availability and security.
- Ensuring adequate virus protection is present on the servers.
- Ensuring all existing IT equipment and software is up to date and fit for purpose and fully functional.
- Ensuring that storage is maintained at reasonable levels.

Staff are responsible for:

- Adhering to the email and Internet policy.
- Immediately informing the IT contractor of any virus detection alerts or spam email.
- Immediately reporting any weaknesses or breaches as soon as they become aware of them.
- Validating and authenticating information retrieved via email and/or from the Internet before it is used for business purposes.
- Ensuring that they log out of the Internet once they have completed their search.
- Ensuring that all e-mail that they send outside the SWDC has the SWDC e-mail disclaimer displayed.
- Users must not share their password, user identification or other secure information.

## 7 Recommended Practices for Retention and Disposal of E-Mail and Internet Material

The person who has the most responsibility for the topic covered should print or file the following:

- Messages which formerly would have resulted in a file note being made.
- Messages that contribute to a greater understanding of significant documents / events.
- Formal communications between employees, for instance, minutes and submissions.
- Messages requesting, authorising or commenting on the expenditure of money or other resources, or any action involving such expenditure.
- Messages containing instructions of a significant nature, including notifications of changes of policy, and establishment of precedents.

Delete without filing the following:

- Routine, short term messages.
- Non-work material, and circulated material sent for information purposes only.

Keep the amount of electronic mail stored in the system to a minimum. That is, always empty deleted items on exiting, save important sent mail and / or attachments, and review e-mail messages on a regular basis.

# 8 SWDC Website

## 8.1 Introduction

The SWDC website has been established as a mechanism for communicating key information with ratepayers and other stakeholders.

Group Managers are responsible for the quality and integrity of the information on the website. The policies and guidelines for the use of the website are designed to ensure that SWDC staff are aware of their responsibilities and roles and appropriate usage.

## 8.2 Scope

These policies and guidelines will apply to all SWDC staff and contractors assigned access rights to the website.

## 8.3 Policy

a. The use of the website is intended exclusively for work undertaken for or by the SWDC.
b. Access to the website is confined to SWDC staff and approved contractors working for the SWDC.
c. Staff must agree to the policies and guidelines.
d. Sensitive or confidential information must not be exchanged via the website.

## 8.4 Responsibilities

SWDC Staff:

- Adhere to the policies and guidelines for website use and information disclosure.

SWDC Management:

- Provide and assure the quality of content for inclusion on the website.
- Copyright on internal and external publications must be clearly identified and adhered to.
- Standard quality controls should apply to information loaded onto the website.
- Develop and disseminate polices and guidelines for the use of the website.

IT contractor:

- Manage the infrastructure for website access and usage, including security.
- Manage user identification and authorisation.

Website Developer (contractor):

- Maintain the structural integrity of the website.
- Training and support to users where needed and approved.

# 9 Facsimile and Telephone Policy

All staff must use facsimiles and telephones including mobile phones in a manner which is consistent with the SWDC standards of conduct and communication and as part of the normal execution of an employee's responsibilities.

In addition, as public servants, we are expected to maintain high standards of ethical and professional behaviour which is not only defensible, but must be seen to be beyond reproach.

## 9.1 Appropriate Use

Staff must at all times comply with the law governing the use of telephones and facsimile equipment and should be aware that certain improper uses could constitute a criminal offence.

In addition to the requirements laid down by law, the *SWDC* prohibits the use of *SWDC* facsimiles or telephones for:

- Obscene or objectionable communications.
- Harassment.
- Conducting gambling or distribution of "chain letters".
- Conducting any illegal activities.
- Soliciting for personal gain or profit or conducting any personal commercial or commercially related activities.

## 9.2 Personal Use

The SWDC incurs the cost of the telephone system and facsimile machines in order to conduct official business. They are not provided for personal use and, because such personal use incurs an unplanned cost for the business, it is a privilege. Occasional and brief personal use is permitted, provided that the calls are local and no long distance charges are incurred. For this purpose SWDC defines the local area as including the SWDC Boundaries.

Private toll calls, including local calls to mobile telephones, charged to the SWDC are prohibited (except in circumstances set out below). Any such calls must be made "collect" or utilising a calling card or the transfer charges facility. In the event of an emergency situation where it is not possible to utilise such services an employee may, with prior approval from a group manager, manager or team

leader, place a private toll call provided arrangements are made immediately thereafter to ascertain the costs and make reimbursement to SWDC.

## 9.3 International Toll Calls

Any international telephone calls for official purposes must be approved in advance by immediate Manager.

## 10 Mobile Phones

Personal use is permitted within the package provided. Expenditure outside this will need to be reimbursed by the employee to SWDC.

## 11 Breach of Policy

Any breach of this policy, either in terms of not observing prohibitions, limits on personal use or requirements to receive appropriate authorisation is "misuse or unauthorised use of SWDC property". As such it constitutes misconduct under SWDC's discipline and dismissal policy.

## 12 Monitoring Rights

SWDC will at the discretion of the Chief Executive or a member of the Management Team, monitor, access, retrieve, read and disclose communication as necessary to verify compliance with this and other policies, in particular to detect and investigate inappropriate use. SWDC may also access communications as necessary to meet urgent business needs or when the employee is unavailable and timing is critical.