



# **Policy Manual - HOGF**

## **Information Technology Policy**

---

**2021**

**Welcome to our Policy Manual**

Please take the time to familiarize yourself with these policies. Hopefully you will find them fair, easy to read, and understandable. Should you have any questions please ask.

You will always find the most recent version of this Policy Manual on the website.

Please complete the acknowledgement and return to me.

Many thanks.

.....

McClean Northey  
Executive Officer

## Receipt and Acknowledgment of Policy Manual

I confirm that I have received and read a copy of our Policy Manual.

I understand that the policies described in it are subject to change from time to time.

I also understand that I will be consulted before significant changes are made and that I will have an opportunity to review and comment on these changes.

---

\_\_\_\_\_  
Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

## **Information Technology Policy**

Instructions about the use and care of information technology (IT) in the workplace including computers and telephones

### **User skills**

Where you are required to use an IT system including software or database as a significant part of your work role and you require training then please notify your supervisor. Unskilled use of IT systems can create errors or downtime which could be embarrassing or expensive for the organization.

### **Passwords**

Each device (laptop, desktop, iPads, mobile phone, PDA) should be protected by a password which prevents unauthorized use.

Each system-user will be provided with a password for server access.

You are responsible for controlling how your password/s is used, and if it is shared. Where a password is shared (for example to a technician for repair purposes) then the password should be changed immediately afterwards.

### **Computer Software (Unauthorised Copying)**

- As a license-holder rather than an owner of software we cannot authorize the copying of software.
- You must use the software only in accordance with the software publisher's license agreement.
- If you know of any misuse of software or related documentation within the Organization, then you must notify management immediately.

### **Use of telephones for private calls**

Personal telephone calls should be kept to a minimum and should not interfere with your job duties. Incidental and occasional personal use of company phones is permitted, but information and messages stored in these systems will be treated in the same way as other digital information. The Executive Officer may request reimbursement of personal calls made on company phones where appropriate.

### **Use of social media**

Each staff member is expected to maintain the principles of appropriate communication when using social media, online communication, or blogs whether during work hours on a personal electronic device, or outside work hours on a personal electronic device.

Online communication that is considered unacceptable includes, but is not limited to, communication that:

- Refers to confidential information owned or held by the organization;
- Is defamatory;
- May be construed as discriminatory or bullying;
- Bullies, harasses, discriminates or vilifies work colleagues;
- Includes abusive status updates and/or blogs that criticize work colleagues, ridicules, and/or breaches their employment obligations in public ways; and
- Publicizes or comments on workplace disputes.

A staff member that engages in online communication to make disparaging comments about the organization, management, colleagues, members, clients and/or supporters may be subject to disciplinary proceedings possibly including termination of employment as per these policies.

A staff member may not establish a social media site, website, blog or other online communication purporting to be a representative of the organization without the express permission of the Executive Officer.

### **Internet and email**

Incidental and occasional personal use of the organization's computer systems is permitted, but information and messages stored in these systems will be treated in the same way as other digital information.

Electronic communications may not be used to:

- solicit for commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations;
- create any offensive or disruptive messages (messages which contain sexual implications, racial slurs, gender-specific comments, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability); nor
- send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

We must be able to respond to service needs and evidentiary requests for electronically-stored information. Therefore, we must, and do, maintain the right and the ability to enter into any of these systems and to inspect and review any and all data recorded in those systems.

The Executive Officer or their designated representative may access, review and disclose such information at their discretion.

Given our right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. The Executive Officer will review any request for access to the contents of an individual's computer, voice mail, or electronic mail prior to access being made without the individual's consent.

#### **Disciplinary provisions**

Staff members who don't follow this policy may be disciplined under the Staff Disciplinary Policy.