Information Technology

Policy and Procedure Manual

Table of Contents

Introduction

The Highland Community College IT Policy and Procedure Manual provides the policies and procedures for selection and use of Information Technology within the business which must be followed by all staff. It also provides guidelines Highland Community College will use to administer these policies, with the correct procedure to follow.

Highland Community College will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Technology Hardware Purchasing Policy

Policy Date: 07/01/2018

The policy for Technology Hardware Purchasing should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money, and where applicable, integrates with other technology for the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

Procedures

Purchase of Hardware

The purchase of all business desktops, laptops, mobile devices, servers, network, and computer peripherals must adhere to this policy. **All computer hardware, software, and mobile device related purchases MUST be approved by or done through Highland Community College IT department.**

Purchasing desktop computer systems

The desktop computer systems purchased must be able to run Windows 10 Pro, Windows 10 Enterprise, or Max OS version and integrate with existing eco-system.

The desktop computer systems must be purchased as standard desktop system bundle and must be by manufacturer Hewlett Packard (HP) or Apple.

The desktop computer system bundle for regular class lab must include:

All-in-One Desktop

- Desktop screen of 23.8” (24 inch)
- Keyboard and mouse must be wired

The minimum capacity of the desktop must be:

- 1.5GHz –gigahertz.
- 4GB RAM
- 500 HDD / 128 SSD
- Intel Core i5 or AMD
- Dual-core processor
- 1 USB port
- 1 HDMI port
- 802.11a/b/g/n/ac

The desktop computer system bundle for Mac lab must include:

All-in-One Desktop

- Desktop screen of 23.8” (24 inch)
- Keyboard and mouse must be wired

The minimum capacity of the desktop must be:

- 1.5GHz –gigahertz.
- 4GB RAM
- 500 HDD / 128 SSD
- Intel Core i5
- Dual-core processor
- 1 USB port
- 1 HDMI port
- 802.11a/b/g/n/ac

The Mac desktop computer system must include the following software provided:

- Office 2016
- Endpoint Protection
- Google Chrome
- Java 8
- .NET 4.7.x
- Adobe
- Silverlight
- Shockwave
- VLC Player

- Dameware Mini Remote Control
- Notepad++
- Custom software configuration as needed per region.

Any change from the above requirements must be authorised by the Director of Information Technology.

All purchases of desktops must be supported by basic 1-year manufacturer warranty and be compatible with the business's server system.

Purchasing portable computer systems

The purchase of portable computer systems includes laptops, notebooks, iPads, and tablets.

Laptops and notebooks computer systems purchased must be able to run Windows 10 Pro or Windows 10 Enterprise version and integrate with the existing eco-system.

Laptops and notebook computer systems purchased must be by manufacturer Hewlett Packard (HP).

iPads and Surface Pro tablets purchased must be able integrate with the existing eco-system.

iPads and Surface Pro tablets systems purchased must be by manufacturer Apple, Inc. or Microsoft respectively.

The minimum capacity of laptop and notebook portable computer system must be:

- 1.5GHz –gigahertz.
- 4GB RAM
- 500GB HDD / 128 SSD
- Intel Core i5 or AMD
- Dual-core processor
- 1 USB port
- 1 HDMI port
- 802.11a/b/g/n/ac

The portable computer system must include the following software provided:

- Office 2016
- Endpoint Protection
- Google Chrome
- Java 8
- .NET 4.7.x
- Adobe

- Silverlight
- Shockwave
- VLC Player
- Dameware Mini Remote Control
- Notepad++

Any change from the above requirements must be authorised by the Director of Information Technology.

All purchases of all portable computer systems must be supported by basic 1-year manufacturer warranty and be compatible with the business's server system.

The **minimum** capacity of iPads and Microsoft Surface tablets computer system must be:

Apple iPad

- Screen size iPad 9.7 inches
- A9 chipset
- 4GB RAM
- 32GB SSD
- 1 USB port
- 802.11a/b/g/n/ac wireless networking

Microsoft Surface

- Screen size 12.3 inches
- Intel core i5 chipset
- 4GB RAM
- 128GB SSD
- 1 USB port
- 802.11a/b/g/n/ac wireless networking

All iPad and Surface tablet computer systems must include the following software provided:

- Subject to approval by Highland Community College IT department.

Any change from the above requirements must be authorised by the Director of Information Technology.

All purchases of all portable computer systems must be supported by basic 1-year manufacturer warranty and be compatible with the business's server system.

Purchasing server systems

Server systems can only be purchased by the Director of Information Technology or Systems Administrator.

Server systems purchased must be compatible with all other computer hardware in the business.

All purchases of server systems must be supported by 24x7 service support and 4-hour response onsite support warranty every year and be compatible with the business's other server systems.

Any change from the above requirements must be authorised by the Director of Information Technology

Purchasing computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives, etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorised by the Director of Information Technology.

All purchases of computer peripherals must be supported by basic 1-year manufacturer warranty and be compatible with existing computer systems.

Any change from the above requirements must be authorised by the Director of Information Technology.

Policy for Getting Software

Policy Date: 07/01/2018

The policy for Getting Software should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for the purchase of software for the business to ensure that all software used by the business is appropriate, value for money, and where applicable, integrates with other technology for the business. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures

Request for Software

All software, including types of non-commercial software such as open source, freeware, etc. here must be approved by the Director of Information Technology prior to the use or download of such software.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased or approved by the Director of Information Technology.

All purchased software must be purchased from reputable software sellers.

All purchases of software must be supported by basic 1-year manufacturer warranty and be compatible with HCC servers and/or hardware system.

Any changes from the above requirements must be authorised by the Director of Information Technology.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from the Director of Information Technology must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the business's hardware and software systems.

Any change from the above requirements must be authorised by the Director of Information Technology.

Policy for Use of Software

Policy Date: 07/01/2018

The policy for Use of Software should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the business to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights and terms of all software licences will be followed by all employees of the business.

Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of the Director of Information Technology to ensure these terms are followed.

Systems Administrator is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

Highland Community College is to be the registered owner of all software.

Only software obtained in accordance with the Getting Software policy is to be installed on the business's computers.

All software installation is to be carried out by Highland Community College IT department.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the Getting Software policy is to be used within the business.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of the Director of Information Technology.

Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.

Unless express approval from the Director of Information Technology is obtained, software cannot be taken home and loaded on an employees' home computer

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from the Director of Information Technology is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the business and must be recorded on the software register by the Highland Community College IT department.

Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to the Human Resource Manager, for further consultation, reprimand action, etc. The illegal duplication of software or other copyrighted works is not condoned within this business and the Director of Information Technology is authorised to undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to Eileen Gronniger, HR Manager, for further consultation, reprimand action, etc.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Director of Information Technology immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to the Human Resource Manager, for further consultation, reprimand action, etc.

Bring Your Own Device Policy

Policy Date: 07/01/2018

The policy for Bring Your Own Device should be read and carried out by all staff members of Highland Community College.

At Highland Community College we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to Highland Community College's network and equipment. We encourage you to read this document in full and to act upon the recommendations.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and computers for business purposes. All staff who use or access Highland Community College's technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Current mobile devices approved for business use

The following personally owned mobile devices are approved to be used for business purposes:

- Apple products such as iPhone, iPad, and smartwatches
- Android products such as smart phones, tablets and smartwatches
- Notebooks / Laptops

Mobile devices for business use

Personal mobile devices can only be used for the following business purposes:

- Accessing company email
- Business internet access
- Business telephone calls

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business sensitive information to the device. Sensitive information includes for example intellectual property, student records, employee details, or other sensitive information, etc.

- Not to use the registered mobile device as the sole repository for Highland Community College's information.

- To make every reasonable effort to ensure that Highland Community College's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all devices should be password protected.

- Not to share the device with other individuals to protect the business data access through the device

- To abide by Highland Community College's internet policy for appropriate use and access of internet sites etc.

- To notify Highland Community College immediately in the event of loss or theft of intellectual property, student records, employee details or other sensitive information on the device

- Not to connect USB memory sticks from an untrusted or unknown source to Highland Community College's equipment.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Exemptions

This policy is mandatory unless Highland Community College IT department grants an exemption. Any requests for exemptions from any of these directives, should be referred to the Highland Community College IT department.

Breach of this policy

Any breach of this policy will be referred to Eileen Gronniger, HR Manager, who will review the breach and determine adequate consequences, which can include but not limited to disciplinary action or termination of employment.

Indemnity

Highland Community College bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify Highland Community College against any and all damages, costs and expenses suffered by Highland Community College arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by Highland Community College.

Information Technology Security Policy

Policy Date: 07/01/2018

The policy for Information Technology Security should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through locks, coded access, and keypads.

It will be the responsibility of the Director of Information Technology to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the Director of Information Technology immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad, tablets etc. will be the responsibility of the employee who has been issued with the laptop, notepads, iPad, tablets etc. Each employee is required to use secure and complex passwords and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the Director of Information Technology will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All laptop, notepads, iPad, tablets etc. when kept at the office desk are to be secured.

Information Security

All sensitive, valuable, or critical business data are to be backed-up.

It is the responsibility of the Systems Administrator to ensure that data back-ups are conducted daily and the backed up data is kept secured in Highland Community College datacentre onsite or offsite.

All technology that has internet access must have anti-virus software installed. It is the responsibility of Network Administrator to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be, include but not limited to disciplinary action or termination of employment.

Technology Access

Every employee will be issued with a unique identification code or password to access the business technology and will be required to set a complex password for access every 180 days.

Each password must meet the following requirements:

- Uppercase character
- Lowercase character
- Numbers 0-9
- Non-alphanumeric characters such as (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

and is not to be shared with any employee within the business.

The System Administrator is responsible for the issuing of the initial password for all employees.

Where an employee forgets the password or is 'locked out' after five attempts, then the Systems Administrator is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

Employees are only authorised to use business computers for personal use such as internet usage, checking personal email.

It is the responsibility of Director of Information Technology to keep all procedures for this policy up to date.

Information Technology Administration Policy

Policy Date: 07/01/2018

The policy for Information Technology Administration should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the business.

Procedures

It is the responsibility of Highland Community College IT department to ensure that all software installed and license information are kept secured and maintained. It must record the following information:

- What software is installed on every machine.
- What licence agreements are in place for each software package.
- Renewal dates if applicable.

The Director of Information Technology is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by the Director of Information Technology

Highland Community College IT department is responsible for maintaining adequate technology spare parts and other requirements including laptop chargers, mice, keyboards, batteries, video cables, and others as approved by the Director of Information Technology.

A technology audit is to be conducted annually by HCC IT department to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to the Director of Information Technology.

Website Policy

Policy Date: 07/01/2018

The policy for HCC Website should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website.

Procedures

Website Register

The website register must record the following details:

- List of domain names registered to the business
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

The keeping the register up to date will be the responsibility of the Director of Information Technology

The Director of Information Technology will be responsible for any renewal of items listed in the register.

Website Content

All content on the business website is to be accurate, appropriate and current. This will be the responsibility of appropriate Content managers of Caffeine.

All content on the website must follow business or content plan objectives.

The content of the website is to be reviewed annually.

The following persons are authorised to make changes to the business website:

- Authorized Content Managers and Administrators of Caffeine.

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the business.

IT Service Agreements Policy

Policy Date: 07/01/2018

The policy for IT Service Agreements should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the business.

Procedures

The following IT service agreements can be entered into on behalf of the business:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of business software
- Website design, maintenance etc.

All IT service agreements or repairs must be reviewed by the Director of Information Technology before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Vice President of Finance & Operations. If cost exceeds five thousand dollars then the agreement must be approved by Highland Community College Board of Trustees.

The Director of Information Technology is responsible for all IT service agreements, obligations and renewals to be recorded and placed in secured location.

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by the Director of Information Technology.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, the Director of Information Technology should review before the renewal is entered into. Once the agreement has been reviewed and

recommendation for execution received, then the agreement must be approved by the Vice President of Finance & Operations. If cost exceeds five thousand dollars then the agreement must be approved by Highland Community College Board of Trustees.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to Highland Community College President who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Policy Date: 07/01/2018

The policy for Emergency Management of Information Technology should be read and carried out by all staff members of Highland Community College.

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the business.

Procedures

IT Hardware Failure

Where there is failure of any of the business's hardware, this must be referred to Highland Community College IT department immediately.

It is the responsibility of Highland Community College IT department to

- Capture data at the time of failure
- Contain the damage and minimize risks

in the event of IT hardware failure.

It is the responsibility of Highland Community College IT department to undertake tests on planned emergency procedures annually to ensure that all planned emergency procedures are appropriate and minimize disruption to business operations.

Virus or other security breach

In the event that the business's information technology is compromised by software virus, malware, ransomware, etc. such breaches are to be reported to the Network Administrator immediately.

The Network Administrator is responsible for ensuring that any security breach is dealt with within 2 hours to minimise disruption to business operations.

Website Disruption

In the event that business website is disrupted, the following actions must be immediately undertaken:

- Director of Information Technology notified
- IT department notified
- Web host provider notified
- Check configuration in web hosting company. Any issues found contact the provider.
- Internal issues contact Systems Administrator

Version History

Version	Change Description	Date	Author
1.0	Placed in new policy	July, 2018	Marc Jean