



University of the
Highlands and Islands
Highland Theological
College

Oilthigh na Gàidhealtachd
agus nan Eilean
Colaiste Dhiadhachd
na Gàidhealtachd

2017

ICT Service A Guide for Staff and Students

Highland Theological College UHI

ICT Service

August 2017

Contents

Welcome to the ICT Service Guide	2
Your Entitlement.....	2
ICT Support for Students.....	3
ICT Support for Staff.....	3
Contacting the ICT Service	3
UHI and Out of Hours Helpdesk.....	4
Software Provision	4
Home Use Software	5
Microsoft Office	5
Autodesk Education Community	5
Sophos Anti-Virus Software	5
Open Source Software	5
Useful Links	5
Student Policies.....	6
User Credentials and Network Password Policy	6
Acceptable Use Policy	6
Other Applicable Policies	7
Staff Policies.....	8
User Credentials and Network Password Policy	8
Other Applicable Policies	8
General ICT Password Controls.....	8
Frequently Asked Questions	10

Welcome to the ICT Service Guide

The purpose of this guide is to provide our users with an overview of the Information & Communication Technology (ICT) resources available at Highland Theological College UHI, as well as the kind of support we can offer our users. The Highland Theological College UHI ICT Technician provides and/or supports:

- The computer on your desk or in the classroom
- Communications (video-conferencing, telephony, fax and email)
- ICT Security
- Local and Wide Area Networks
- Server infrastructure
- Storage
- Applications and Software
- Printing and Copying
- Multimedia and Presentation (interactive whiteboards, audio and video)
- Mobile devices (mobile phones and tablets)

The majority of the computing equipment at the college is in the form of Windows 10 based PCs and various printers and scanners throughout the college.

Your Entitlement

As a Highland Theological College UHI student or staff member, you are provided with:

- A personal user account for access to any computer on the UHI network
- A UHI email account
- Access to the Internet.
- Access to a wide variety of UHI software, both on a college computer and at home via the MyUHI service
- Secure personal storage on UHI servers, accessible from any college computer and at home via MyUHI
- Access to printing and copying facilities
- Access to the UHI wireless network for *bring your own devices* (BYOD)



ICT Support for Students

The ICT Technician is here to help you with any college-related ICT issue. This includes:

- Logon issues
- Network issues, such as access to your home drive and Internet access
- PC faults or issues, be that hardware or software
- Printing problems

Outwith the college, first line support is provided by the ICT Service Helpdesk which can be reached on 01463 279150.

Although we endeavour to support students whenever possible, we regret that we cannot provide support for student-owned devices.

ICT Support for Staff

The ICT Technician provides first line support for HTC Staff and UHI Staff based at HTC on all UHI ICT issues or requests, redirecting queries to the UHI Helpdesk when necessary. As well as offering the same support that we provide to students, we can also assist with:

- Software installations and upgrades
- Using college equipment – interactive whiteboards and projectors
- General software queries – email, Microsoft Office etc.

Generally speaking, if you have a technical query, we will try our best to help you with it.

Contacting the ICT Service

The ICT Technician can be contacted in a number of ways: email; Lync; telephone and by dropping by.

E-mail - mike.day@uhi.ac.uk

Telephone - 01349 780207

Location - Downstairs, at the back of the college, adjacent to the car park door

Helpdesk Hours

Monday to Thursday - 09:00 to 17:00

Friday - 09:00 to 16:00

(there may be a reduced service during college holidays)

UHI and Out of Hours Helpdesk

The UHI helpdesk is available to all UHI students and staff. They provide first line support for all queries and problems with any service provided by LIS, including Video Conferencing.

Monday to Friday - 09:00 to 17:00

The Out of Hours helpdesk is run in partnership with our service partners at NorMAN. This is open at all times when the UHI Helpdesk is closed, including overnight, weekends and holiday periods.

Monday to Thursday - 17:00 to 09:00

Friday through to Monday - 17:00 to 09:00

Plus all UHI closure periods

Phone (Internal) - Ext. 150

Phone (External) - 01463 279150

Email - uhihelpdesk@uhi.ac.uk

Software Provision

College Computers differ slightly depending on the needs of the department but all share a common base build. This includes:

- Microsoft Office Professional 2016
 - Word
 - Excel
 - Outlook
 - Access
 - PowerPoint
 - Publisher
 - OneNote
- Adobe Reader, Flash Player and Shockwave Player
- Java
- Apple QuickTime
- Sophos Antivirus

The majority of the college PCs also have:

- VLC Player
- Audacity

Department staff are responsible for ensuring that software required by the course is available. If some software seems to have been omitted, students should speak to the department staff who will bring it to the attention of the ICT Technician.

By using MyUHI from a home computer, users will have access to various software packages remotely, including Microsoft Office. Details can be found on the UHI website at <http://www.uhi.ac.uk/en/lis/myuhi>.

Please note – The default browsers used by the Highland Theological College UHI are Internet Explorer 11 on Windows 10. Many of the web-based systems are designed to run in these browsers and we therefore recommend that you use them. You are free to use any other (if installed) but they will not be supported by the ICT Technician.

Home Use Software

Microsoft Office

Staff can purchase Office Professional at a discounted price by visiting <http://www.uhi.ac.uk/en/lis/software-downloads/> and following the instructions.



Students can download Microsoft Office for FREE! by visiting <http://www.uhi.ac.uk/en/lis/software-downloads> and clicking on the Microsoft Home Use tab.

Note: Student copies of Microsoft Office will expire when the student completes their studies with UHI/HTC.

Autodesk Education Community

Staff and students can sign up and freely download Autodesk software by visiting http://students.autodesk.com/?nd=download_center and following the online instructions.

Sophos Anti-Virus Software

The UHI has a licencing agreement with Sophos which includes home use rights for staff and students.

Open Source Software

Open source software is software that is made available along with the source code so that anyone can modify the code to alter the software to meet their needs or improve it. Some software is publicly available such as Mozilla Firefox, Linux and Open Office among others. These can all be installed on home PCs and Open Office can be especially useful if money is tight.

- <http://www.openoffice.org/> - Download Open Office, a usable alternative to MS Office
- <http://sourceforge.net/> - Repository of open source software
- <http://opensourcewindows.org/> - List of the best open source software for windows



Please **do not** try and download and install any software on college PCs or laptops. Unauthorised software installations (even open source or “freeware”) are in breach of the relevant ICT security policies.

Useful Links

UHI Connect: <http://connect.uhi.ac.uk>

UHI Webmail: <http://webmail.uhi.ac.uk>

Blackboard: <http://www.blackboard.uhi.ac.uk>

HTC: <http://www.htc.uhi.ac.uk>

MyUHI: <http://myuhi.ac.uk>

UHI: <http://www.uhi.ac.uk>

Mahara: <http://uhi-mahara.co.uk>

UHI Intranet: <http://intranet.uhi.ac.uk>

ICT Security Policies

At Highland Theological College UHI we take security very seriously and enforce certain rules regarding passwords and security policies on college computers. We also have some unenforced policies that all users must comply with to strengthen the security of our network as a whole.

Student Policies

The following policies apply to student accounts:



User Credentials and Network Password Policy

- **Usernames** – College students are assigned a username in order to log in to the college computers when they enrol. Returning students will normally retain the same username. The username will be a string of numbers and cannot be changed.
- **Passwords** – When a student account is created, the password will initially be the student's date of birth in the format DDMMYYYY. When first logging on this should be changed to a secure personal password to prevent unauthorised access to the account.
- **Password Complexity** – Passwords must contain a minimum of 5 characters (6 or more is recommended) and should consist of upper and lower case letters and at least one special character or number. For example "Security1" would be acceptable. Passwords however should not consist of recognisable names or be easy to guess.
- **Password Changes** – Passwords should be changed at least once every term, and the new password should not have been used within the current academic year.
- **Temporary Credentials** – Under certain circumstances the ICT Technician may approve student use of generic user credentials. These are issued either on a per-site basis (i.e. learning centres) or for certain applications (e.g. ECDL exams). These accounts have specific (and usually limited) access rights, and must only be used at the specified site or for the intended purpose. Under normal circumstances students must log on using their own credentials.
- **Unattended Computers** – It is essential that students log off when leaving computers unattended even if they intend to return to that PC, e.g. at break times. If a computer is to be left unattended for a short period of time and it cannot be logged off (i.e. running a process or downloading course material) it must be locked (using the Win + L keys). If a computer is locked and the student does not return any unsaved work will be lost.

Acceptable Use Policy

Highland Theological College Computing Facilities

The Highland Theological College UHI computing facilities are provided to facilitate each student's work for educational or training purposes. **All students are expected to check their email accounts regularly for communication from college staff.**

Use for other purposes, such as personal email or recreational use of the World Wide Web or Usenet News, is a privilege, not a right, and may be withdrawn. Any such use must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the College into disrepute.

Subject to the following paragraphs, the College computing facilities may be used for any legal activity that is in furtherance of the aims and policies of the User and or User Organisation.

Unacceptable Use

The College computing facilities **may not** be used for any of the following:

- The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- The creation or transmission of material which is designed to or likely to cause annoyance, inconvenience or needless anxiety.
- The creation or transmission of defamatory material.
- The transmission of material such that this infringes the copyright of another person.
- The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks.
- Deliberate unauthorised access to facilities or services accessible via the College computing facilities.

Or **deliberate activities** with any of the following characteristics:

- Wasting staff effort or networked resources, including time on end systems accessible via the College computing facilities and the effort of staff involved in the support of those systems; corrupting or destroying other users' data; violating the privacy of other users; disrupting the work of other users.
- Using the College computing facilities in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).
- Continuing to use an item of networking software or hardware after College staff have requested that use cease because it is causing disruption to the correct functioning of the College computing facilities.
- Other misuse of the College computing facilities or networked resources, such as the introduction of 'computer viruses'.
- Copying or using unlicensed copyright software.

Where the College computing facilities are being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College computing facilities.

Other Applicable Policies

- Janet Acceptable Use Policy
- UHI IS Acceptable Use Policy
- UHI IS Computer Operations Policy
- UHI IS Information Classification Policy
- UHI IS Protection Against Malicious Software Policy

Copies of these documents are available from the UHI website at <http://www.uhi.ac.uk/en/lis>

Staff Policies

The following policies apply to staff accounts:



User Credentials and Network Password Policy

- **Username**s – Unless specifically requested and approved, staff usernames will adhere to the UHI AD format, i.e. partner identifier; two digit number; users' initials.
- **Password**s – A basic password will be assigned to the user for initial login, upon which time the user will be forced to change the password to a more secure one; access to network resources, including email, will be unavailable until the initial password has been changed.
- **Password Complexity** – Passwords must contain a minimum of 5 characters (6 or more is recommended) and should consist of upper and lower case letters and at least one special character or number. For example "Security1" would be acceptable. Passwords should not consist of recognisable names or be easy to guess.
- **Password Changes** – Passwords should be changed at least once every ninety (90) days, and the new password should not have been used within the past five changes.
- **Unattended Computers** – When leaving a computer for even a short period of time, the account should be locked to prevent unauthorised access. If leaving a computer for a prolonged period of time the user should log out altogether. A locked screensaver will activate after 10 minutes of inactivity but this is only a secondary security feature and should not be relied upon.

Other Applicable Policies

- Janet Acceptable Use Policy
- UHI IS Acceptable Use Policy
- UHI IS Computer Operations Policy
- UHI IS Information Classification Policy
- UHI IS Protection Against Malicious Software Policy

Copies of these documents are available from the UHI website at <http://www.uhi.ac.uk/en/lis>

General ICT Password Controls

The following general controls apply to all users of the college network:

- By logging onto any area of the UHI network; including college computers, email and the college intranet, you are agreeing to abide by the UHI ICT security policies.
- User Credentials are issued to individuals and the disclosure of these credentials to another party is strictly prohibited. However, in the event of there being a support incident, the ICT Technician (or UHI Support Staff) may ask for the current user credentials to investigate the reported fault. In this event the user will be required to change their password as soon as the fault is resolved.
- Passwords should not be recorded and/or stored in an easy to retrieve manner, i.e. on a post-it note attached to the monitor.
- If there is any suspicion that a password has become known by an unauthorised third party, the authorised user must change their password immediately and notify their tutor (for students) or line manager (for staff) as well as the ICT Technician (or UHI Support Staff).

- It is the responsibility of each user to ensure that password controls are adhered to as no enforced policies are applied to the Active Directory network (with the exception of the 5 character minimum password length, staff screen savers and lock times).
- In the event of an investigation into a potential breach of this policy, users should be aware that a reasonable presumption will be made that the owner of an account is responsible for any material accessed or created on a password protected system, or the sender of any e-mail associated with the user account.
- The Highland Theological College ICT Technician or UHI LIS reserves the right to impose a mandatory password reset to any or all users on the network if it is considered that a breach of these controls has occurred.

The Highland Theological College ICT Technician (or UHI Support Staff) reserves the right to disable the account of any user who is found in breach of the Highland Theological College or UHI ICT security and acceptable use policies. Any such breach will be immediately reported to a relevant tutor or line manager.

Frequently Asked Questions

How much email storage do I have?

A. All UHI Office 365 email accounts have 50GB of online storage.

How do I access my email from home?

A. You can access Office 365 via the Outlook Web App using any browser from <http://outlook.com/uhi.ac.uk> (It is recommended you use Internet Explorer 8 or above to get the best experience). If you're using Internet Explorer you must enter your username prefixed with `uhiad\` - i.e. `uhiad\ht01xx` for staff or `uhiad\01001234` for students. This is not required from any other browser (Firefox, Chrome, Safari, etc.).

Can I access my email from a mobile device?

A. Yes. Please use the "connect your mobile device" link on this page: <http://webmail.uhi.ac.uk>

Can I access my documents and files from home?

A. Yes, log on to <http://my.uhi.ac.uk> and you will find a fully functional UHI desktop with access to your various network drives, as well as UHI software (Office, etc.).

Can I use my own laptop or mobile device in the College?

A. Yes, but only through the UHI Wi-Fi service. On no account must you attempt to connect a personal device to the college wired network. You can find full details on connecting to the UHI Wi-Fi service with your own device here: <http://www.uhi.ac.uk/en/lis/wifi>

Can I use my USB memory stick or portable hard drive on College computers?

A. Yes, but you do so entirely at your own risk, and the ICT Technician (or UHI Support Staff) will not be held responsible for any loss of data. You must also be aware that any introduction of malware or computer viruses to the college network via a removable device will be treated as a serious incident and a breach of ICT security policies.

Is my network data backed up?

A. Yes. All data on the College file servers are backed up nightly using eVault.

Is it possible to recover accidentally deleted files?

A. Usually this is possible, providing they were saved to a network location and remained there for at least one night. Files created then deleted the same day will not be recoverable. The same applies for files saved only to removable media. In the first instance contact the UHI Helpdesk to see if recovery of deleted files is possible in your case.

Why are some websites blocked?

A. UHI operates a web filtering policy to protect users from inappropriate or offensive content. If you think that a particular website should be available please click the more information link on the block page and follow the instructions to request a website review.

Why is my user account showing up as expired?

A. Student accounts are set to expire at the end of the last academic year of their studies. If a student enrolls on a new course they will usually use the same student ID, but the network account is not automatically enabled. Additionally, the ICT Service periodically runs user account housekeeping and all user accounts that have not been used in the last 180 days are disabled. Contact your tutor, the ICT Technician (or UHI Support Staff) to have your account enabled.

Why can't I send large files using email?

A. The Office 365 email system has an attachment limit of 25MB per email, either as a single file or multiple attachments.