FFURFLEN MANYLION
IDENTIFICATION FORM /FRONTSHEET

TEITL : *TITLE:*	**ICT USAGE – Learners**
UWCH-GYFARWYDDWR A CHYFRIFOLDEB: *RESPONSIBLE EXECUTIVE DIRECTOR:*	*Corporate Services*
PWRPAS: *PURPOSE:*	*This is Grŵp Llandrillo Menai's* guide for Learners to provide information on ICT facilities available to Learners and to make Learners aware of their responsibilities when using ICT within Grŵp Llandrillo Menai.
CYFATHREBU *COMMUNICATION*	*Grŵp Portal*
PWLLGOR / GRŴP MONITRO: *COMMITTEE / GROUP RESPONSIBLE FOR MONITORING:*	*JCC* *Tîm Strategol*
CYMERADWYWYD GAN: *APPROVED BY:*	*Kath Coughlin*
DYDDIAD CYMERADWYO *APPROVAL DATE:*	
DYDDIAD ADOLYGU *REVIEW DATE CYCLE:*	*Annual - 2020*

Version: 11.1
Last Updated: May 2019
Reference: Aidan Sheil, Sharon Millership

Purpose of this document

This document has been written as a guide for learners, and staff, to provide information on ICT facilities available to learners and to make learners aware of their responsibilities when using ICT within Grŵp Llandrillo Menai. This document operates within the framework of the equality and diversity related policies of the College. ICT (Information Communication Technology) includes all computer, network and technology facilities at the college. This document will be reviewed on an annual basis or more frequently if required, in line with any changes within the Grŵp.

General

A disclaimer is displayed on all college networked computers as follows:

Accounts are provided for college course work only, and as stated in the disclaimer, by logging into the machine Learners are agreeing that any activity on the system may be monitored.

Learners must:

- Ensure they have their ID card and lanyard on at all times when on college campus
- Ensure they logout of the system when they leave their PC unattended
- Ensure no one knows their password, they must not give their password out to anyone and not let anyone else use their network account for any reason
- Make all reasonable efforts to ensure that their network access remains secure and report any breaches or suspected breaches of security to ICT Services immediately

Network Account and Data Storage

Account login and passwords will be issued by the course tutor. The student password is assigned centrally and cannot be changed unless requested to the ICT Services Helpdesk (based in Dinerth Block at Rhos site, ext 1460). If a student forgets their password they can request it by showing their ID card to a course tutor, member of IT workshop staff or ICT Services.

Learners with individual network accounts will have 500mb of data storage by default plus unlimited storage through Google Drive.
This can be increased if deemed necessary by request of the student's tutor.
This storage area is seen in My Computer as drive **h:** - no one else has access to this area and this is the area where all work should be saved. There is a folder called **docs** and a folder called **config** on all student h: drives – these folders are required by the system and should not be renamed or deleted, as this will stop some programs from running. Many applications will default to save work to the h:\docs folder but learners can also create additional folders to organise their work.

Work should not be saved to the c: drive as it will be lost when the user logs out of the network. Work should also not be saved directly to removable media such as floppy disks or USB pen drives - it should be saved to the network h: drive first and then be copied to these devices.

Grŵp Llandrillo Menai uses Moodle and Google Classroom for it's Virtual Learning Environments (VLE). Access to this facility will be provided to learners by the course tutor/s.

Student accounts and data will be kept for 12 months, if not used for a 12 month period they will be deleted.

Email
The Learner's External E-mail address will be learneridnumber@gllm.ac.uk

Learners can access their email accounts within college using the icon called "GLLM Email" under the Programs folder, and externally at the following URL

mail.gllm.ac.uk

They can also follow the link on the college web site for Student email.

If a student forgets their e-mail password it can be reset by contacting the ICT Services Helpdesk through their tutor.

For all network account queries Learners must show their ID card.

Internet access

Internet access is provided primarily for college coursework . All Internet access is monitored and web sites deemed inappropriate are blocked from being accessed. If a student feels that a web site is blocked incorrectly they can request access through their tutor who will pass this request on to ICT Services.

Printing and consumables

Learners need to be environmentally responsible, use onscreen print preview facilities, only use printing facilities when necessary, and avoid printing multiple copies.

From September 2011 a print monitoring facility called Papercut, was implemented across all sites. This will monitor and log all printing on the college network. Printing facilities are provided for College academic purposes only and not for personal use.

Learners will be allocated a £20 print credit in September and a further £20 credit in January and April. Learners will not be able to go into a negative balance, if they do not have enough credit to print, the print job will not print and they will get a message to say they have an insufficient balance.

Learners will be able to pay for additional print credits at college finance offices and other agreed staffed areas.

Course Tutors can also request individual learners or groups of learners have additional printing credited allocated if deemed necessary.

Account Responsibilities

Abuse of the E-mail
College policy does not allow the following when using the e-mail system:

- Use of the E-mail system when and where requested not to do so by any member of staff
- Sending of multiple E-mails. (A single E-mail to a number of individuals or distribution lists)
- Sending abusive or threatening E-mails
- Sending E-mail that may bring the colleges name into disrepute
- Distribution of potentially offensive graphics as attachments
- Distribution of games and other software as attachments
- Use of other people's E-mail accounts, or attempted use of other people's e-mail accounts, either by proxy or by obtaining their passwords
- Sending of excessive personal e-mails
- Other abuse not listed

Abuse of Internet access
College Policy does not allow the following when using the Internet:

- Excessive web surfing for personal use
- Downloading of any software
- Attempting to deliberately access offensive or unauthorised sites, for example pornography, violence, hacking and other sites banned by Grwp policy
- Attempting to deliberately access sites containing information which could be described as "hacking tools"
- Playing games or attempting to run peer to peer activities

- Online anti-social behaviour eg bullying, harassment, trolling, posting of offensive messages or comments
- Other abuse not listed

Abuse of Software, Systems, Hardware and Network facilities

College policy does not allow the following when using any college ICT facilities:

- The use or attempted use of unlicensed software, systems or hardware
- The installation or attempted installation of any software, systems or hardware
- The copying or attempted replication of college software
- Any attempt to use any software not available through the "Application Launcher" Window
- The copying, transmission or submission of material such that this infringes the copyright of another person or organisation
- Use of college printing facilities for non college business related purposes
- Use of other people's login accounts, or attempting to use other people's login accounts
- Attempting to use hardware or software to capture network traffic, e.g. information on users login ids, passwords or network activity
- Attempting to access any unauthorised data area on the network
- Saving of inappropriate material to any college PC or network area e.g. music files, games, graphics, photos and other files not related to college work
- The creation or transmission of any offensive, obscene or indecent images, data or other materials, or any data capable of being resolved into obscene or indecent images or material
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- The creation or transmission of defamatory material
- The introduction of viruses from external sources
- Any attempt to re-configure or change any software settings on any PC
- Any attempt to remove attached devices or attach unauthorised devices to a machine or to the college network, or any attempt to move or disconnect any college ICT equipment e.g. PC, printer, telephone
- Corrupting or destroying other users' data
- Violating the privacy of other users
- Disrupting the work of other users
- Other abuse not listed

Consequences of any abuse:

Any abuse of ICT Facilities is regarded as a serious breach of the College's disciplinary code and will lead to action being taken against the learners involved as follows:

- Accounts will be disabled whilst the alleged abuse is investigated
- Abuse of the system may lead to learners being subject to the College disciplinary procedures

A user who breaks this agreement will be dealt with in accordance with the College disciplinary code. Sanctions include:

A reprimand
Withdrawal from the College
Suspension from the College
Exclusion from the College

Contacts

Any queries about the content of this document should be taken up with the learner's course tutor in the first instance.

Any queries with regards to the use of any ICT system should first be taken up with the course tutor. There is also a drop in IT workshop facility at each site where support is available.

Any queries about passwords or any possible breach of network security should be reported to the course tutor and/or to ICT Services as soon as possible.