ICT USER ACCEPTANCE POLICY

FOR STUDENTS

CONTENTS

1 INTRODUCTION

1.1 WHAT THIS POLICY IS FOR

This policy has been created to define acceptable use of Eden Education ICT services, equipment and systems, and the protection of data and sensitive information held within them.

Every person studying at Eden Education should be aware that unacceptable use is strictly prohibited and could lead to appropriate disciplinary or legal action.

Eden Education has taken account of the guidance of the Information Commissioner in preparing this policy and in particular 'The Employment Practices Data Protection Code, Part 3: Monitoring at Work'.

1.2 WHAT THIS POLICY COVERS

This policy applies to all learners ("Users").

The policy applies to all forms of ICT equipment, systems and data including:

- Hardware such as Servers, PCs and laptops, removable media such as CDs, DVDs, memory sticks, smartphones, tablets etc and all data held on these devices.
- Data transmitted over communications lines including internal and external networks and the Internet.
- Email received or sent including their attachments.
- Files, images and other data stored on local, network or removable drive.

Students should be aware of how and why any checks on their ICT system use are carried out. That information is set out in this document.

2 EQUIPMENT USE AND MONITORING

Students may be provided with access to standard ICT hardware (desktop pc, printer etc) upon the commencement of their course with Eden Education.

The ICT systems are provided for educational use only, limited personal use which does not impact business performance or the functionality of the ICT system is permitted.

All data and documents held within the Eden Education ICT environment is the property of the organisation and subject to IT and Data Protection policies.

Students may be given Internet access, as deemed necessary, to carry out their studies. As such, there should be no expectation of privacy in the use of the system. Users of Eden Education's Internet facilities waive any right to privacy in anything they view or access using the organisation's systems.

Eden Education's ICT Department will determine the appropriate firewall protection for all offices. Firewall implementation helps in the exclusion of undesirable web sites.

Telecommunications (Lawful Business Practice), (Interception of Communications), Regulations which came into force on 24 October 2000 set out the circumstances whereby service providers (in this case Eden Education) may intercept communications without the consent of students. These are:

- Recording evidence of business transactions.
- Establishing the existence of facts.
- Policing and enforcing company policies.

- Receiving or redirecting employee messages during absence.
- Preventing or detecting crime, fraud or corruption.
- Monitoring standards.
- To investigate or detect unauthorised use (such as more than minimal personal use).
- Ensuring the security of the system.
- Preventing computer viruses.

3 NOTIFICATION OF SECURITY INCIDENTS

If you become aware of any breaches of information security then you must record them and report them immediately to your tutor and the ICT Service Desk as appropriate.

Serious incidents, such as Data Protection issues or the loss (suspected or actual) of hardware and/or confidential data should be reported immediately to the ICT Service Desk, who will cascade the incident to the relevant authority to deal.

If you see any unusual or suspicious occurrences on a PC or laptop then you must report this immediately to the ICT Service Desk in case there has been a virus or hacker attack. Do not continue using the suspect workstation.

4 USER IDS, PASSWORDS AND ACCESS

Where you have been allocated personal User IDs and passwords, you should keep the passwords safe and should not share them with any other individuals.

If you need to delegate your responsibility to other individuals, there are always ways in which this can be done without divulging your own details to another individual. Please contact the ICT Service Desk for further advice.

Never write your passwords down or record them in any supporting documentation.

Security regarding access to your PC is of paramount importance. Ensure that you lock your PC by pressing the **CTRL, Alt** and **Delete** keys simultaneously and then **Enter** or the **windows key** and **'L'** before walking away from your desk. You will be held accountable for actions performed using your User ID including emails that have been sent or released using the Corporate Spam Filtering System.

You should not attempt to use or view any systems or data for which you are not authorised. If you are unsure about your access rights, please contact your tutor or a member of the ICT Department.

You must not attempt to gain access to secured areas containing computer equipment, communications equipment or computer media unless you have been expressly authorised. Unsecured equipment should also be treated with care and should not be tampered with unless you have the permission and knowledge to use the equipment.

5 EXTERNAL DEVICES

All portable removable media which has not been provided by Eden Education is **NOT** to be connected to the Eden Education Domain without permission from your tutor. Such devices, although this list is not exhaustive, are listed below:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.

- Memory cards in SD, Compact Flash, Memory Stick, or any related flash-based supplemental storage media's card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods/tablets with internal flash or hard drive-based memory that support data storage function.
- PDAs, mobile phone handsets, tablets and smartphones with internal flash or hard drive-based memory that support data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access.

6   LEAVERS POLICY

All accounts will be disabled for the first 30 days after the course end date, and the retention of data will be in adherence with the Data Protection Policy unless otherwise specifically requested. All leavers should remember that any data is the property of Eden Education and they should not have retained any 'private' information on their equipment or within their Eden Education mailbox.

7   EMAIL ACCESS, USAGE AND MONITORING

Remember that access to the Eden Education email system is provided solely as a tool for undertaking the business of Eden Education.

7.1 EMAIL MONITORING

Email services may be monitored and if necessary intercepted.

Eden Education reserves the right at any time to monitor and/or retrieve the contents of any message sent or received, irrespective of whether the use is legitimate or not, to assist in the investigation of alleged wrongful acts or to comply with legal obligations.

All users must be aware of their responsibilities and obligations to others under the terms of the Data Protection legislation. Care must be exercised in respect of data held about other people both inside and outside the organisation for operational or any other purpose.

Please be aware that email communications can be presented as evidence in a court of law and are legally binding.

Inappropriate use of Eden Education email can result in disciplinary action, which in serious cases can result in summary dismissal.

Users must be aware that email can be deemed in law to constitute publication and therefore the standard laws of libel apply. Incorrect or inappropriate use can cause a variety of problems ranging from criminal offences to legal claims made against individuals and Eden Education.

The intellectual property rights, design, patents, copyrights and confidentiality of mailed information remains vested with Eden Education.

7.2 IMPORTANT RULES FOR EMAIL USAGE

Email (with any associated attachment or hyperlink) must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory, pornographic or obscene, defamatory or libellous or

any other material which is otherwise abusive or contains illegal content prohibited by law or regulation or which brings Eden Education into disrepute or which contravenes Eden Education's policies and procedures.

It should be noted that emails are discoverable documents in legal actions and may be used in evidence under the Regulation of Investigatory Powers Act (2000). You must not transmit statements about another party which may be deemed defamatory or libellous.

Email as a form of correspondence can be used as a standard contract confirmation. As such, users must ensure that the information, tone and context are correct prior to sending to ensure that individuals do not enter into contractual agreements unwittingly.

Requests made by third parties to release the organisation's email address book must first be agreed in writing by the ICT Department.

Care should be taken in opening email attachments from unknown or unsolicited individuals/companies. Should users be unsure about the contents of any attachment or email, then the email and its contents should be deleted.

If users do open inappropriate or unsolicited material that may cause concern, they must report this immediately to their line manager.

Should users receive an email that has been incorrectly delivered they should contact the sender of the message by re-directing the message back to that person. If that message contains confidential information, they are not permitted to disclose or use that information.

Staff must not use personal email addresses for business use.

Staff should be aware of the "Phishing" techniques used by fraudsters and should take steps to verify the validity of content not received from trusted corporate email accounts. It is the user's responsibility to report such phishing incidents to ICT immediately.

7.3 ACCESS TO EMAIL ACCOUNTS
In some circumstances it will be necessary to access the email account of a former member of staff, e.g. to gain access to work related information that the user has stored on their email account and not copied to their manager/team/colleagues prior to leaving.

If a member of staff is absent from work for any reason (sickness, annual leave) Eden Education ICT may grant access to the user's mailbox as directed by their manager or Eden Education HR.

8 ACCESS TO THE INTERNET
8.1 IMPORTANT RULES FOR INTERNET USAGE
Eden Education provides internet access to assist with the aims of our business and to make your work easier.

No user may download or install Internet based software without the written approval of the ICT Department.

8.2 SOCIAL NETWORKING
Access to social networking within the Eden Education network will only be granted in exceptional cases and when the requirement has also been agreed by Eden Education's Digital Media Manager or Senior Management.

Any use of personal social networking sites to bully staff or students or bring the name of Eden Education into disrepute will be considered as grounds for instant expulsion.

8.3 INSTANT MESSAGING

The only forms of instant messaging permitted within Eden Education are those provided by the ICT department which are limited to Lync or Skype for Business accounts based on Eden Education owned email addresses.

9 VIRUS PROTECTION

Virus/Malware infection is a serious and ever-increasing threat to an organisation's network and data. Eden Education IT provides virus/malware protection in various forms. These run in the background so in general you should not have to take any proactive action to protect the systems from virus attacks. You should not interfere with the installation or running of any anti-virus software. If you observe anything suspicious with your computer or the IT systems then you should report this to the ICT Service Desk.

10 DATA ENCRYPTION

Eden Education has put in place measures to ensure that sensitive and confidential data is stored and transmitted in an encrypted format.

All personal/sensitive information should be handled in this way and utilities or options provided for encrypting data should be enabled and not tampered with under any circumstances.

11 BACK-UPS

All data stored on network drives and in cloud storage are automatically backed-up on a regular basis. Data held locally on laptop and desktop computers is not backed up.