Appropriate use of Information Technology Policy

This Policy and your responsibilities

1. Who and what this policy applies to.

This policy applies to every student and member of staff who uses any of the IT Services provided by the Caspian School of Academics (CSA). The policy applies whether you are on campus or working from home, a workplace or at distance. The policy applies to your use of School equipment and School services as well as your own equipment when you use it on School business.

Your responsibilities.

You must read this policy and keep to the rules and guidelines set out within it. These exist to protect you and to ensure that you learn safely and get the most from School IT systems.

2. Your agreement and disciplinary action if you break it.

Your agreement to stick to the rules in this policy are set out and confirmed when you sign your Student Learner Agreement or your contract of employment.

Monitoring and disciplinary action.

What you do online when using the School network and what you access and store on the School network is monitored and logged. If you break the rules of this policy, you may face disciplinary action and potentially in the most serious circumstances Police investigation.

Reporting of issues.

If you suspect that someone else is breaking these rules or at risk, students must share their concerns with their tutor and staff with the IT support team (in confidence if necessary) who will make sure that issues are investigated and support services are informed as required to support the user.

3. What the School does to protect you.

CSA does lots to help everyone to stick to the rules. The School does a lot in the background to protect everyone from threats that might arise online. Here are some of the things that the School does:

a. Internet

Being a School that caters for a wide range of learner ability, age and interest, we try to give access to as much of the Internet as appropriate whilst keeping our learners safe. To protect our learners and our staff, our IT security systems automatically block access to thousands of inappropriate web sites. Such web sites might promote racial discrimination or hatred, for example. If anyone need access to a blocked web site e.g. to research racial discrimination for a social sciences project, students should speak to their tutor who may be able to arrange access, and staff should speak to IT support.

b. Personal Details.

We do not publish anyone's personal details and School staff must protect everyone's privacy.

c. Anti-virus software.

Software that detects and deals with computer viruses is on every School computer and server. This antivirus software is continually updated to ensure your protection.

d. School Computers.

The software on School computers (including desktop computers, laptops and tablets) has been configured to prevent tampering. You must not attempt to install or permanently reconfigure software such as the operating system, security or application software.

4. What you must do to protect yourself and others.

Connecting to the School network

Users of the School's network must not connect any equipment using an Ethernet cable. Users are permitted to connect their own devices to the School's wireless('Wi-Fi') network only. Users are expected to ensure that any device attached to the School network has the latest security patches installed and up to date Antivirus software installed. The School reserve the right to scan devices automatically or manually and block access if these terms are not met.

Fair usage if a user is found to be consuming excessive bandwidth the access will be suspended pending investigation. Using School network to share content and copyright materials is not acceptable and would result in further action.

Phishing (Emails or websites trying to get bank account details).

Beware of links in E-mails and think before you click on them. They may look very real but are not really from BT, Microsoft, Banks. Do not put any details in to this kind of site.

Phone calls from these companies can also be fake and are trying to get hold of details or control of your device. Examples: you have won a lottery for which you have never brought a ticket: helping get money out of another country: payments for medical treatments. The purpose is to obtain bank details so your accounts can be emptied.

Use of network tools etc.

The unauthorised use of network tools and changes to the School network is not allowed. If anyone needs to use network tools, monitor networked devices or install and configure servers and control systems then they should be provided with an isolated network to facilitate learning or work without risking the availability and security of network resources for other users.

Help and guidance.

At the start of their course of study or at the start of their employment, staff and students will be shown how to access the School systems and how to use them safely. They will also have opportunity to ask questions about this policy. Always seek help if you have questions or concerns about using the School's IT systems – IT Services and Student Services have a lot of experience and are keen to help you.

Protect your personal details.

Going online exposes you to thousands of people who want to trick you into giving them access to your personal details. Never give your personal details (including name, age, address, phone number, credit card or bank account details) or a photo of yourself (or anyone else) to any stranger on the Internet. Do not lend anyone your student card or divulge your network password, even to your best friend: this is a disciplinary offence.

Protect your money.

You will almost certainly receive scam email messages, even though the School uses sophisticated security systems. Scam emails can look very convincing and often promise you money or goods in return for your personal details such as your email address or even your bank account details. Always delete these scam emails, and do not reply. If you are in doubt, then ask someone else to take a look – but do not give out your personal details.

If you buy anything online, make sure that the seller advertises contact details including a phone number, and that it has good reviews. Any payment by credit card should take you to a secure site for entry of details. If you do not know what one of these looks like, then ask someone to check for you before you enter any personal details.

Protect your reputation on social networking sites.

The School accepts that you may use social networking sites such as Facebook in your own time. Although we are not responsible for these sites and cannot control them, we strongly recommend that you take care when allowing others access to your Facebook or similar sites. Make sure your privacy settings are correctly configured to keep you safe. Think carefully before you post text and photos because even if you remove later they may have already been forwarded elsewhere, at which point you lose control of who sees them.

Remember that what you might share with a close friend could be interpreted very differently by a stranger. Your reputation is precious and easily damaged – look after it.

Be careful what you say about others on social networking sites.

Do not use your social network to spread lies about people, places or organisations. Publishing lies online - even amongst friends on social networking sites - can result in legal action being taken against you. Check the terms and conditions of social networking sites and use them for interacting with friends in your own time and not anti-social or illegal activity.

School use of social networking sites

The School cannot be responsible for social networking sites outside its own network and provides a 'virtual learning environment' (Moodle) as a safe and secure alternative.

However, the School recognises that special features of some social networking sites might invite you to join a social network site to communicate and collaborate with other students or colleagues. You are strongly recommended to read and abide by all rules of such sites. Do not use these sites to vent negative feeling against other learners, staff or the School: what you say can be seen by others and you will be held accountable. Use the proper procedures if you want to complain about something.

CSA School Identity Card

When you enrol or are employed at CSA you are given an identity card that enables you to gain entry to School buildings and classrooms as well as access to resources such as the library.

Do not lend you card to anyone. Your card is for your use only and you may become liable for any issues that might arise should you let somebody else use it.

Protect your network username and password

When you enrol for are employed at CSA you are given a username and temporary password to enable you to connect to the School network. You are required to create a new password when you first login to the School IT systems.

It is very important that you protect your network password in order to maintain your privacy and to ensure that you are not accused of wrongdoing should somebody else break these rules whilst pretending to be you.

Here are a few do's and don'ts:

Do:

- Use your username and password when you log in to the School network. Never use somebody else's username and password. If the person before you have forgotten to log off, you must log them off the School network and log in as yourself.
- Always log off the network when you have finished work, otherwise you might be held responsible for what the next person does in your name.
- Change your password if you suspect that someone has learned it by watching you type it in.

Do not:

- Give your username and password to anyone else inside or outside the School.
- Write your username and password down. Just remember them – it's much safer.

Email – use it sensibly.

Keep your email messages short and to the point. Get into the habit of using a greeting, adding a description to the 'Subject' field and finishing your message with your name and contact details. Do not use email to criticise others or to 'shout' at people (avoid using lots of capital letters for emphasis). Remember that email messages can be easily circulated to people you know (and those you do not know) and could even be quoted against you in court, so choose the words you use carefully.

Students should tell their tutor if they accidentally visit an unacceptable web sites mistake

Sometimes you might accidentally visit an inappropriate web site that should have been blocked by our automated security systems (occasionally these systems fail to identify an inappropriate web site, perhaps because it has just appeared or recently changed name). The School understands that mistakes happen, but you should still tell your tutor as soon as possible because otherwise the School's monitoring systems might prompt a formal investigation. Telling us also means that we can block such sites from other users.

If you need to access web sites that are normally blocked.

Some coursework may require research into subjects that are normally blocked as unacceptable. For example, you might need to research the use of illegal drugs for a project. In such cases, your tutor must contact IT Services beforehand to request a temporary exception to the rules. If you are at all uncomfortable about the areas that you need to access and how these might be at odds with this policy, please seek assurance from your tutor,

5. What you must not do

For clarity, this guidance is sub-divided into unacceptable 'content' (things you must not look at, download, publish, or communicate) and unacceptable 'activities' (things you must not do).

Unacceptable Content

You must not seek, view, download, publish, transmit or communicate content that is:

- illegal

- threatening
- offensive
- abusive
- libellous (untrue or unfair comments about someone which will harm their reputation)
- harassing
- targeted at those with 'protected characteristics'
- discriminatory
- pornographic
- sexist
- racist
- unlicensed for use within the Caspian School

and/or which relates o:

- terrorism and extremism
- cults
- dating
- controlled drugs
- bullying
- gambling
- criminal activity (including software hacking)
- social chat, jokes or chain mail that is not related to your course social groups
- promotion of any kind of discrimination
- personal business (such as any private work that you do)
- encouraging violence, or unlawful conduct.

You must not:

- do anything which may bring the School into disrepute
- commit illegal activity or activity which breaches any School policy
- provide access to facilities or information to those who are not entitled to have it
- use School facilities to bully, harass, intimidate or otherwise cause alarm or distress to others
- attempt to undermine the security of the School's facilities, including hacking or undertaking any unauthorised penetration testing or vulnerability scanning of any School systems
- pretend to be other users by using their network username and password
- try to access the network anonymously (so you cannot be identified)
- write or introduce viruses or other programs designed to cause harm
- introduce unauthorised equipment e.g. modems, other active equipment, monitors etc. which
- could adversely affect network performance and put sensitive data at risk
- waste resources or introduce insecurities
- tamper with workstation addresses, settings or software
- use School IT facilities purely for private, social or personal business use within timetabled study time
- use School IT systems to advertise material that may provoke or offend others, such as extremism or hate crime
- use School systems to attack other systems, sites, organisations or individuals

- use School systems to transmit details about other people that you do not have permission to pass on
- use School systems to re-publish material that is copyright (owned by others)
- send e-mail messages or phone messages which are abusive, harassing or include unacceptable content, swearing and threatening language
- download software without School permission or introduce software for which you hold a personal home license without first checking suitability with IT Services and if the software may be legally used on business premises
- download or use games or access games over the network, other than software installed and/or approved for learning purposes
- download copyrighted information for storage, re-transmission or re-use including copyright images, text, data, music and video
- create, store or transmit defamatory or obscene material (where there be genuine need to access such material e.g. during a criminal investigation, prior permission for controlled access must be obtained from the Director of Operations or the Director of Communications)
- advertise the email address or location of any other person without their permission
- create and transmit bulk e-mail messages that could be construed as 'spam' email
- subscribe any other person to any online facilities without that person's consent
- publish 'example' or 'fictitious' material about courses or the School that may be confused with genuine School-published materials
- fail to comply with a request from an authorised person for you to change your password
- fail to report any breach, or suspected breach of information security
- fail to comply with a request from an authorised person to stop any activity which is detrimental to the operation of the School's facilities.

6. Personal use of School systems

Personal Use of IT Facilities

The School accepts limited personal use of its IT facilities outside timetabled class time or worktime. This might include research, personal finance, family appointments/communication, social networking etc. so long as:

- it does not interfere with your study or anyone else's study or work
- it does not contravene any School policies
- it is not excessive in its use of School resources.

Those who use School IT facilities to make purchases, pay bills or conduct online banking or similar activities do so at their own risk. The School cannot be held responsible for any direct or indirect losses sustained by those using its IT facilities for personal transactions.

Personal Mobiles and devices

Phones, tablets, smartphones and any other personal devices should only be used in personal time and not during timetabled class time unless permitted by your tutor. In exceptional circumstances, such as home emergencies, you should check with your tutor who can make allowances.

The School is not responsible for third party mobile networks on which devices such as mobile phones and smartphones operate and cannot intercept or block calls. Do not use your mobile phone, smartphone and/or tablet to abuse others or to send anything anonymously. If you receive messages or voice mail or anything else that upsets you, ask your tutor or any member of staff for support -

there are trained staff within School who will offer you support and keep you safe. Whilst the School is not responsible for activity that occurs on third party networks, it will report serious incidents to relevant telecommunications providers.

7. Review of this policy

This policy will be reviewed annually by the Head of IT and approved by the School Senior Management Team.

8. Documents related to this policy

- Student Learner Agreement
- Anti-Bullying and Harassment Policy
- Safeguarding and Prevent Duty Policy and Procedures
- Equality and Diversity Policy.
- Harassemnt and Sexual Misconduct Policy Condition E6