SWANSEA COLLEGE
Building foundations for your future

Information and Communications Systems Policy

Policy statement

Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor their use, and the action we will take in respect of breaches of these standards.

In particular, remember that you are representatives of the College and all communication through our systems (whether by telephone, e-mail or otherwise), must be conducted in an appropriate manner.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Who is covered by the policy?

This policy covers all individuals working at all levels and grades, including senior staff, officers, Principals, employees, consultants, tutors, contractors, trainees, home workers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this policy). Third parties who may access to our IT and communication systems are also required to comply with this policy.

The scope and purpose of the policy

This policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones and voicemail. It also applies to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

Misuse of IT and communications systems can damage the business and reputation of the college.

All staff must comply with this policy at all times to protect our IT and communications systems from unauthorised access, misuse, and harm. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Personnel responsible for implementation of the policy

The Principal has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to our operations also lies with the Principal.

The Principal will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining our core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

All senior staff members have a specific responsibility to operate within the boundaries of this policy, ensure that all staff understand the standards of behaviour expected of them and to take action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of our electronic communications systems or equipment should be reported to the Principal. Questions regarding the content or application of this policy should be directed to the Principal.

Equipment security and passwords

Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office, they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting a member of staff in reception.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Principal. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to the Principal and return any equipment, key fobs or cards.

Staffs who are issued with a laptop, PDA or Blackberry must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Systems and data security

Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

Staff should not download or install software from external sources without authorisation from the Principal. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff should seek advice.

We monitor all e-mails passing through our system for viruses. Staff should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .exe). A manager should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this policy. We also reserve the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

Staff using laptops or wi-fi enabled equipment must be particularly vigilant about its use outside the office and take precautions from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

Credit and debit card payments

The college uses a secure onetime payment system.

When taking payments in person or via the telephone, the card details should be entered directly onto the online system and the payment processed immediately.

Card details are not written down, whether electronically or on paper, and are not stored.

If sensitive card details are sent to the college by a customer or other party, they should be processed immediately and then deleted. Confirmation should be sent to the customer that this has taken place.

E-mail etiquette and content

E-mail is a vital business tool, but as an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate method for a particular communication. Correspondence with third parties by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling and use an out-of-office response when away from the office for more than a day. They should endeavour to respond to e-mails marked "high priority" within 24 hours.

Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform the Principal.

Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

In general, staff should not:

- send or forward private e-mails at work which they would not want a third party to read;
- send or forward chain mail, junk mail, cartoons, jokes or gossip;
- contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;
- agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;
- download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- send messages from another worker's computer or under an assumed name unless specifically authorised; or
- send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.
- staff who receive a wrongly-delivered e-mail should return it to the sender.

Use of the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors.

Staff should, therefore, not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time.

Extremism and prevent programme

Staff and students are not allowed to access any extremist or pro-terrorist websites or other forums. Any staff member who does access these will be subject to out disciplinary procedures. Anyone who becomes aware that others (staff, students, volunteers etc) who is visiting / using sites like this should inform the Academic Manager or Principal in confidence. This is part of our duty to safeguarding vulnerable people and forms part of the prevent programme (see SWANSEA COLLEGE Whistleblowing Policy).

Personal use of systems

We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused, and we reserve the right to withdraw our permission at any time.

The following conditions must be met for personal usage to continue:

- use must be minimal and take place substantially out of normal working hours;
- personal e-mails must be labelled "personal" in the subject header;
- use must not interfere with business or office commitments;
- use must not commit us to any marginal costs; and
- use must comply with our policies including the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure.

Staff should be aware that personal use of our systems may be monitored (see paragraph 10) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see paragraph 11). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

Monitoring of use of systems

Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, is continually monitored by the IT department. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

A CCTV system monitors the exterior of the building and interior of the building 24 hours a day. This data is recorded.

We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (and this list is not exhaustive):

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts; or
- to comply with any legal obligation including our duties under the prevent programme.

Inappropriate use of equipment and systems

Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with our rules, policies and procedures (including this policy, the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure). See paragraph 9, Personal use of systems.

Misuse or excessive use or abuse of our telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by:

- participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):
- pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

- offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
- a false and defamatory statement about any person or organisation;
- material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
- confidential information about us or any of our staff or clients (which you do not have authority to access);
- any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
- material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or senior staff involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

Use of Social Media Policy

About this policy

This policy is in place to minimise the risks to our business through use of social media.

This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Personal use of social media

- Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.
- You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

- You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- You must not express opinions on our behalf via social media, unless expressly authorised to do so by the Principal. You may be required to undergo training in order to obtain such authorisation.
- You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.
- You are not permitted to add business contacts made or students during the course of your employment or indeed students of the College to personal social networking accounts.

Any misuse of social media should be reported to the Principal.

Guidelines for responsible use of social media

You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out in paragraph 3.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with the Principal.

If you see social media content that disparages or reflects poorly on us, you should contact the Principal.

Breach of this policy

Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Monitoring and review of this policy

The Principal shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

Staff are invited to comment on this policy and suggest ways in which it might be improved by contacting the Principal.

The effectiveness of this policy and associated policies, as well as our training provisions is evaluated at the annual internal audit.