Farnborough College of Technology	**IT Security and Acceptable Use Policy**
Owner	Data Protection Officer
Approval by Corporation	Not applicable
Date reviewed:	May 2018
Date for next review:	May 2019

Introduction

Farnborough College of Technology recognises the importance to its business of effective information security management and has therefore undertaken to protect its key business information assets by working to a programme designed to meet the requirements of general information security standards. This covers all aspects of information handling, including information asset management, physical and technical security measures, staff awareness and training, incident management and audit.

Further information

If you need further information concerning this document, or our information security policies in general, please contact the IT Manager.

Reporting Breaches

Please report any breaches (or suspected breaches) of the Information Security policy to the Data Protection Officer or the IT Department immediately.

- All security breaches are assessed by the DPO and if necessary the DPO will convene a meeting of the college's senior management team.
- Please do not put off reporting any security incident. All reports will be treated in confidence.
- Failure to comply with these policies may result in disciplinary action as detailed within the college’s policies and procedures

Employee Security Awareness Training

As an automated process, intended to ensure that all staff understand the huge importance Farnborough College of Technology puts on security awareness, the contents of this policy are provided to all new starters.

The policy is also sent on an annual basis to remind all staff of the 10 Guiding Principles of security that they must adhere to, to help ensure protection of Farnborough College of Technology’s key business information and manage all data in a confidential manner.

CONFIDENTIALITY & SECURITY

FCOT's 10 Guiding Principles

1 FOLLOW OUR IT STANDARD USAGE GUIDELINES TO BE LEGAL, COMPLIANT & SECURE

All systems are owned by Farnborough College of Technology. If you are provided with a computer as part of your job, or if you use your own computer attached to the college's guest network, you need to be familiar with our policies on computer, email and internet usage.

2 FOLLOW EMAIL GUIDELINES

Email guidelines designed to protect students, staff and the College are provided and should be adopted by everyone that uses College email systems.

3 FOLLOW INTERNET GUIDELINES

Internet guidelines designed to protect students, staff and the College are provided and should be adopted by all staff.

4 FOLLOW SOCIAL MEDIA GUIDELINES

Social Media guidelines designed to protect you, the staff and the College are provided and should be adopted by everyone that uses College internet systems.

5 UNDERSTAND YOUR DATA PROTECTION RESPONSIBILITIES

Please ensure that any personal information is handled in compliance with our Data Protection and GDPR policies.

6 DO NOT INSTALL SOFTWARE ON COLLEGE COMPUTERS

Please do not download and/or install software onto PCs that are connected to the network. If you do need additional software, this should be acquired and installed by the IT team.

7 PROTECT YOUR LOGIN CREDENTIALS

Please look after your system username and password and keep the details confidential. You will be required to change your password every 60 days, or immediately if you suspect it has been compromised.

8 TAKE CARE OF COLLEGE I.T. EQUIPMENT AND RETURN IT WHEN YOU LEAVE

Please take reasonable care of all College equipment and information. Generally, you are expected to take good care of College computers and to keep them safe from damage or theft, especially if they are used outside the office.

9 USE NETWORK STORAGE AND APPROVED APPLICATIONS TO PROTECT DATA

The College provides storage on network shared areas and on OneDrive cloud storage – these are the only approved areas to store personal data and other systems should not be used without express permission from the IT Manager.

10 UNDERSTAND THAT DATA SECURITY IS MORE THAN JUST COMPUTER SECURITY

Please follow good security practices - Clear meeting rooms after use; do not leave confidential documents on printers; be responsible for visitors; mark documents as confidential; and destroy or shred confidential documents.

FOLLOW COLLEGE IT STANDARD USAGE GUIDELINES TO BE LEGAL, COMPLIANT & SECURE

All systems are owned by Farnborough college of Technology. If you are provided with a computer as part of your job, or if you use your own computer attached to the college's guest network, you need to be familiar with your policies on computer, email and internet usage.

- Use of the college's information systems is provided for business purposes only, and not generally for personal, private, or non-business use. Sensible use of email to receive a moderate amount of private correspondence does not constitute misuse of the system but if, however, levels became very high, we would discuss the matter with you.
- Email and permanent access to the internet are provided for business purposes only. Whilst the college accepts moderate and reasonable personal usage*. All communications made by you are in the name of the college. We therefore reserve the right to access, read, and monitor or store any communication made or received by you using the College's computer system.
- All System users are prohibited from using College equipment for any illegal activity
- Creating, viewing, accessing, transmitting or downloading any of the following scenarios will usually amount to gross misconduct (this list is not exhaustive):
  - Sending, receiving or storing offensive, obscene, or criminal material or material which is liable to cause embarrassment to the college - Under the Obscene Publications Act (1994) you can be prosecuted if you have pornographic images on your computer. If you have images, even if they have been sent to you and they have not been opened, this is illegal. Any transfer of pornographic material via the net is also illegal and could result in your dismissal from the college.
  - Using the internet to visit illegal file sharing, obscene or other sites which may put the college at risk of prosecution, civil action, embarrassment or loss of reputation.
  - Using unauthorised software or music or video files or other material in breach of copyright - Respect the copyright or licensing laws that may apply to software, music, images or other materials of any kind, be they digital or hard copy. College information systems must not be used to download, copy, store or transmit material that may violate copyright or license restrictions.
  - Making a false and defamatory statement about any person or organisation OR material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the College's Equal Opportunities Policy or Anti-harassment and Bullying Policy);
  - Distributing confidential information about the College or any of its staff or clients (except as authorised in the proper performance of your duties);

  - Engaging in any other activity which is likely to create any criminal or civil liability (for you or the College).
- You should be aware that electronic data can be retrieved and used to provide evidence of misuse of electronic information, if required, and you should therefore ensure that information passed about competitors, clients or individuals is not defamatory, obscene or discriminatory. You are responsible for the content of email messages. Emails may be disclosed as evidence in any court proceedings or investigations by regulatory bodies.
- The College systems enable monitoring 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, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.
- We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (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 alleged wrongdoing; or
  - to comply with any legal obligation.

If you are uncertain whether a particular use of your computer, email or the internet is allowed, please speak to the IT Manager for clarification

*Personal use of systems

- Email and permanent access to the internet are provided for business purposes only. Whilst the College accepts moderate and reasonable personal usage, all communications made by you are in the name of the College. The College therefore reserves the right to access, read, and monitor or store any communication made or received by you using the College computer system.
- Personal use is a privilege and not a right. It must not be overused or abused. The College may withdraw permission for it at any time or restrict access at its discretion.
- Personal use must meet the following conditions:
  - it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);
  - personal e-mails should be labelled "personal" in the subject header;
  - it must not affect your work or interfere with the business;
  - it must not commit us to any marginal costs; and
  - it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy and Disciplinary Procedure.

  - Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our disciplinary procedure. Misuse of the internet can in some cases be a criminal offence.

FOLLOW EMAIL GUIDELINES

The following Email guidelines designed to protect students, staff and the college are provided and should be adopted by all staff. Please find student email guidelines within the 'Student Use of College Computers, Email, and the Internet' procedure on the Intranet.

- Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.
- Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.
- You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.
- Email should not be used to enter into, change or terminate a contract.
- You should not:
  - send or forward private e-mails at work which you 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 others who do not have a real need to receive them; or
  - send messages from another person's e-mail address (unless authorised) or under an assumed name.
- Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.
- Please take care when using email to avoid potential fraud and phishing attacks, which often involve identity theft. You should not click on links in emails unless you are sure of the source. Be wary of unusual emails from trusted sources.
- Please maintain your inbox ensuring that you are not storing any personnel information if not required
- For any sensitive information being sent outside of the college please ensure it is adequately password protected, and that the password to that file is sent in a separate e-mail

FOLLOW INTERNET GUIDELINES

The following Internet guidelines designed to protect students, staff and the college are provided and should be adopted by all staff. Please find student

Internet guidelines within the 'Student Use of College Computers, Email, and the Internet' procedure on the Intranet.

- Internet access is provided primarily for business purposes only.
- You should avoid using the internet to visit illegal file sharing, obscene or other sites which may put the College or any group College at risk of prosecution, civil action, embarrassment or loss of reputation.
- You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK 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 college 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.
- The College may block or restrict access to some websites at its discretion.

FOLLOW SOCIAL MEDIA GUIDELINES

The following social media guidelines designed to protect students, staff and the College are provided and should be adopted by all staff. Please find student social media guidelines within the 'Student Use of College Computers, Email, and the Internet' procedure on the Intranet.

- This section of the policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram 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 College business in any way.
- Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.
- You must avoid making any social media communications that could damage college interests or reputation, even indirectly.
- You must not use social media to defame or disparage the College, its 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 the College’s behalf via social media, unless expressly authorised to do so by your manager. 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 College performance, or do anything to jeopardise the College’s integrity, confidential information and intellectual property. You must not include College logos or other trademarks in any social media posting or in your profile on any social media.

- The contact details of college contacts made during the course of your employment are confidential information. On termination of employment you must provide the College with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.
- Unless such postings are done in a work context, 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 the College on your profile or in any social media postings, you must state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to students 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 your manager.
- 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 any investigation, which may involve handing over relevant passwords and login details.
- You may be required to remove any social media content that the College considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

UNDERSTAND YOUR DATA PROTECTION REPOSNSIBILITES

Please ensure that any personal information is handled in compliance with our Data Protection and GDPR policies.

Your personal data held by the College

- All the information (including paper files and computer records) the College keeps on you is held under the General Data Protection Regulation (GDPR). You may have access to any information recorded about you within 30 days your request. The College takes full responsibility for the safekeeping of the information and will ensure it is only used for business purposes, The College will keep your data after you have left for 7 years in accordance with legal retention periods. After this time all electronic and paper records will be permanently destroyed.

Personal data you process as part of your role

- The college also processes personal information relating to students and third parties. It is the responsibility of all staff processing such information to ensure that they do so in accordance with the GDPR.

IT Retention and Destruction Policies

- All IT computer assets including servers, laptops and desktop PCs and MACs are recycled in line with industry best practice via an approved recycling company. All hard disks are wiped and data destroyed before any equipment is re-used and all machines that have no residual value are recycled and destroyed in line with WEEE regulations. Computers cannot be resold, given to charity or given to staff as part of severances packages to ensure that data gets fully deleted and destroyed by approved and regulated suppliers.

DO NOT INSTALL SOFTWARE ON YOUR COLLEGE COMPUTERS

Please do not download and/or install software onto PCs that are connected to the network. If you do need additional software, this should be acquired and installed by our IT team.

- Only software that has been approved by the IT Department may be installed on college computers. College computer systems must not be modified or updated without approval from IT management. Please note that we monitor and regularly review installed software on all of our computers.
- The use of downloaded freeware, shareware or other non-approved software is prohibited. Not only does downloaded software present a significant security risk, it could also put the college in breach of copyright law.
- All college computers are supplied with approved anti-virus and patch management software and may also be provided with other security software. You must not disable or re-configure these security tools.
- Employees must not contact suppliers for any IT or telecommunications equipment or service without approval from IT, and are prohibited from installing any devices connected to the college's voice and data networks
- Computers not owned or managed by the college must not be connected to our network without approval from IT management.

PROTECT YOUR LOGIN CREDENTIALS

Please look after your system username and password and keep the details confidential. You will be required to change your password every 60 days, or immediately if you suspect it has been compromised.

- All users of college information systems will be given a unique User ID and password for those systems. You must not share these with anyone and you must not use anybody else's login details to access College computers, phones or networks.
- Passwords will expire and must be changed at least once every 60 days. However, if you suspect your password has been compromised, you must change it immediately.

- Passwords must be no less than 8 characters in length, using at least one uppercase, one lowercase and one non-alphabetical character.
- Passwords must not be written down in an easily accessible place (for example, they should not be displayed on pin-boards or on stickers on your computer or phone).
- College computers are configured with a password-protected screensaver. However, if you are working on a particularly sensitive document on screen, please remember to close it or minimise the application if you leave your desk.
- You should log out and shut down your computer at the end of every day.

TAKE CARE OF COLLEGE IT EQUIPMENT AND RETURN IT WHEN YOU LEAVE

Please take reasonable care of all College equipment and information. Generally, you are expected to take good care of College computers and to keep them safe from damage or theft, especially if they are used outside the office.

- Restricted information, the use or disclosure of which would be contrary to the interests of the college, is to be kept confidential and must only be used for the benefit of Farnborough College of Technology.
- Information is at a high risk of loss or theft when used outside the office. If you take college information outside the office, the following precautions must be taken:
  - All mobile devices must be password-protected to minimise the risk of data theft if the device is lost or stolen.
  - Laptops and other mobile devices should not be left unattended at any time in a public place. During air travel they should always be carried in hand luggage. Overnight, mobile devices should be locked away in a secure location whenever possible.
- The College provides mobile phones which are provided by learner services for borrowing in instances of College trips for example. The invoiced calls are inspected each month and, if excessive and not due to work calls then the College reserves the right to deduct the additional cost from the salary of the person in possession of the phone (after first discussing it with you). If you lose the College phone, please report the loss immediately to our IT manager. Please report the theft or loss to the police so that you have a crime or lost item reference number. If you lose or damage the mobile phone due to negligence, then we may ask you to pay to replace it.
- Please take great care when using a college laptop and make sure it is kept under lock and key when you are not using it. In the event that it is stolen or damaged due to negligence we may ask you to contribute to the cost of replacement.
- When leaving the college, you must return all College equipment - Equipment is the property of the college and only the Principal, Finance Director, Estates and IT Management can assign or re-assign property to an employee. You must not lend College equipment to others.

- If/when you leave the college, you must return any equipment issued to you on or before the last day of work. You must not remove any data, information or other materials of any kind belonging to the college when you leave.

USE NETWORK STORAGE AND APPROVED APPLICATIONS TO PROTECT DATA

The College provides storage on network shared areas and on OneDrive cloud storage – these are the only approved areas to store data and other systems should not be used without express permission from the IT Manager.

- All electronic business information and files should be properly stored on the college's network drives (Currently presented as M:\ & O\ drives) or on OneDrive as this ensures data is secure and available. Computer hard disks (C: or D: drives) are reserved for personal data and will not be backed up by Farnborough College of Technology.
- When working out of the office only take the data you need to work on and transfer it back to the network drives on your return. *No personal data to be taken off site.?*
- It is your responsibility to ensure you are taking adequate backups of data stored on your laptop or another mobile device. For further advice, please contact IT.
- Do not use College equipment as your only source of personal data such as important photographs and music – It is not the responsibility of the College to keep these safe and secure.
- Removable storage devices pose a significant security risk and should be used with great caution. Information stored on removable storage devices or media (such as USB pen drives, external hard drives and mobile phones) is at a high risk of loss due to the portable nature of these devices and media, and the wide range of computers they can be connected to if lost or stolen. Information may only be stored on removable storage devices temporarily to transfer data from one location to another. Once the information has been transferred, it must immediately be deleted from the removable storage device. Each department is provided with a pre-encrypted USB, please use these devices this if you absolutely need to transfer sensitive information by USB
- Everyone should be aware that electronic data can be retrieved and used to provide evidence of misuse of electronic information, if required, and you should therefore ensure that information passed about competitors, clients or individuals is not defamatory, obscene or discriminatory.
- Ensure as far as possible that the information is not readily visible to others – especially when working in public places.
- You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

UNDERSTAND THAT DATA SECURITY IS MORE THAN JUST COMPUTER SECURITY

Please follow good security practices - Clear meeting rooms after use; do not leave confidential documents on printers; be responsible for visitors; mark documents as confidential; and destroy or shred confidential documents.

- If you are expecting a visitor to Farnborough College of Technology, please inform the relevant reception of the name, date and time your visitor will be arriving.
- All visitors should be met in the reception area.
- Be conscious that work being undertaken by the college can be sensitive so please restrict visitor access only to the areas they need to be.
- Although the college has 24-hour security coverage, it is everyone's responsibility to understand and follow all security systems in the building in place at the time. Failure to adequately ensure the security of the building or its contents is a breach of contract.
- The College accepts no responsibility for the loss of any personal items which are brought to work so please lock up anything of value.
- Documents containing information not in the public domain are considered "Restricted"; highly sensitive information should be marked "Team Restricted". Restricted documents include business plans, personnel files, financial data, contracts, strategy documents, student information.
- It is your responsibility to identify Restricted documents, and to classify and treat them accordingly. If you are unsure how to classify documents, ask your line manager immediately.
- Ensure that restricted documents are not left unattended and that they are filed away at the end of every working day.
- If you are disposing of restricted materials, ensure they are destroyed appropriately (for example, paper documents should be shredded).
- Ensure that any files sent to print are picked up from the printer immediately. Likewise, please remember to pick up originals as well as copies from photocopiers.
- If you take documents into a meeting room, make sure that you remove them when you leave. The person convening the meeting should make a check at the end of the meeting to ensure all materials have been removed.