MyTutor www.mytutor.co.uk

Acceptable Use Policy

Security Incident Reporting Quick Reference

Note! Regardless of confidence level, all security incidents must be immediately reported by phone *and* email. So even if the security incident is only potential or suspected—it must still be reported without delay.

Contact by Mail *and* by Phone	**Comment**
dataincident@mytutor.co.uk	Use email *and* phone below
07748644728	The Firm Support Number
“The Firm”/ MyTutor	MyTutor

Document Approval

This document has been approved by the following

Role	**Name**	**Version Details**
CEO MyTutor	Bertie Hubbard	See section 9.4 Version Control, and section 9 Document Control

Contents

1. Overview

MyTutor provides many essential services and business functions which rely on ICT technology resources. The use of ICT resources must be in line with good professional working practices, procedures and must ensure the security and integrity of all MyTutor information and data.

2. Policy Statement

2.1.1. Computer Use

All users of MyTutor's computers must ensure at all times that:

- Authorisation has been provided to use the ICT facilities with a Domain username and password provided by the IT Department.
- User and System account logon passwords are kept private and not shared, displayed or communicated to anyone who does not have a legitimate right to that information.
- MyTutor's information and data is not permanently saved to PC hard drives – in the event of MyTutor's network being unavailable, advice should be sought from the IT Department.
- Sensitive and personal data is not knowingly saved on the PC's hard drive under any circumstances.
- Data and Information saved to portable devices via a PC is only copied to MyTutor approved portable device which is encrypted in accordance with the Encryption Policy.

N.B - Mobile computing devices such as digital cameras and digital dictation devices etc., must not be treated as data storage devices – however, MyTutor accepts that photographs/audio files can also be classed as data and recommends that any photographs/audio files taken are removed from the device(s) and stored on MyTutor network as soon as possible.

- Screens/computers are locked by users when away from the computer.
- MyTutor computer equipment, such as desktops, (with the exception of laptop and CTO authorised for use) are not removed from their location without line management and/or approval from the IT Department.
- Unauthorised, non-standard equipment is not plugged-in or inserted into the computer.
- Software is not installed on MyTutor's IT computer equipment by unauthorised staff (authorised access may include specific duties requiring staff to have administrative access in order to carry out certain job functions) – any software installed must be (or going through the process of being) placed on the approved software list.

- MyTutor’s ICT equipment must not be used to store Personal data such as wedding photos, CV’s, music files etc.
- Computers are not mishandled, wilfully damaged or tampered with in any way – this includes taking off the PC/laptop case cover, or removing of any screws or fixings.
- Any suspiCTOus or unknown equipment near or around PC's/laptops is reported to the IT Department.
- Computers are logged off and shut down when not in use for extended periods (i.e. overnight) and monitors are powered off.

2.1.2. Internet and Email Use

2.1.2.1. Internet

- Personal use of the Internet is allowed but not during working hours. You can use the Internet before you start work, during your lunchtime, or after work.
- You must not use MyTutor's Internet or email systems for trading or personal business purposes.
- If you use the Internet to buy goods or services, MyTutor will not accept liability for default of payment or for security of any personal information you provide.
- Goods must not be delivered to a MyTutor’s address.
- Downloading of video, music files, games, software files and other computer programs - for non-work related purposes - is strictly prohibited. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

Many Internet sites that contain unacceptable content are blocked automatically by MyTutor's systems. However, it is not possible to block all "unacceptable" sites electronically. You must not therefore deliberately view, copy or circulate any material that:

- Is sexually explicit or obscene.
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive.
- Contains material the possession of which would constitute a criminal offence.
- Promotes any form of criminal activity.
- Contains images, cartoons or jokes that will cause offence.

MyTutor records the details of all Internet traffic. This is to protect MyTutor and its employee's from security breaches, including hacking, and to ensure that 'unacceptable' sites are not being visited.

2.1.2.2. Email

Where possible, personal use of email should be in your own time; limited personal use of email during the working day is allowed, but should be restricted to a total of no more than a few minutes to respond to urgent incoming personal email.

Personal use must not, in any way, distract staff from the effective performance of their duties.

Excessive use is not allowed and may result in disciplinary action including loss of your Internet and email access.

You must not use the email system in any way that is insulting or offensive. You must not deliberately view, copy or circulate any material that:

- Is a sexually explicit or obscene
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- Contains material the possession of which would constitute a criminal offence
- Promotes any form of criminal activity
- Contains unwelcome propositions
- Contains images, cartoons or jokes that will cause offence
- Appears to be a chain letter

MyTutor routinely produces monitoring information which summarises email use and may lead to further investigation being undertaken.

2.1.2.3. Security

MyTutor's computer systems are under continuous threat from hackers, virus/malware infections, data and equipment theft. MyTutor must remain vigilant at all times in order to safeguard information and data and to protect the security and integrity of all ICT systems.

Users of all MyTutor's computers and devices must ensure that:

- Computers/devices are not given to any unauthorised persons for safe keeping
- Computers/devices are not left discarded or unattended in public places.
- All portable mobile computing devices and other IT equipment should not be left unattended in any vehicle at any time.
- Computers/devices must be adequately protected from physical damage.
- Computers/devices are not hired, lent or given out without authorisation from the IT Department.
- All Computers/devices which are no longer required or which have reached the end of useful life must be returned via the line manager to the IT Department to be disposed of in accordance with Disposal of ICT Equipment.

2.1.2.4. Antivirus

Any warnings visible on screen from MyTutor's Antivirus/Antimalware software about identified/detected threats from viruses/malware should be reported to the IT Department immediately.

2.1.2.5. Personal Devices

Personal devices which are not the property of MyTutor, including mobile phones, PDAs, digital pens etc., must not be used to record or capture information relating to MyTutor and its services.

2.1.2.6. Breaches of policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to MyTutor's assets, or an event which is in breach of MyTutor's security procedures and policies.

All MyTutor's employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through MyTutor's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of MyTutor.

MyTutor will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

For more information, see Security Incident Management Policy.

All users of MyTutor's ICT facilities must comply with this policy and be aware of the ICT Security Policy.

This document forms part of MyTutor's IS Policy and as such, must be fully complied with.

3. Scope

The scope of this policy extends to all departments, employees, contractors, vendors and partner agencies who use/access MyTutor's ICT facilities.

4. Purpose

The purpose of this Acceptable Policy is to apply acceptable use controls to Information, Information Systems, software Applications, Communication Networks, and CTO, used throughout.

5. Definitions

Term	Description
Information	Any information, data or record irrespective of format, collected, generated or used by a business system or process. Examples include electronic communications, emails, digital recordings such as Call Centre Telephone conversations and CCTV, hard copy (paper) files, photographs, maps, plans, process documentation (code, scripts, etc.) and technical drawings.
Information Classification	Assigning a piece of information to a particular category based on its content
Information [Asset] Owners	Executive and Senior managers who are responsible[1] for managing the acquisition, creation, maintenance, usage and disposal of MyTutor's Information and Information Systems within their assigned area of control
Information Risk	That part of MyTutor's overall risk portfolio which relate to the confidentiality, integrity and availability of information within MyTutor.
Information Security	The ability to protect the confidentiality, integrity and availability of information held by MyTutor, including any sub-contractors and suppliers, from unauthorised use, disclosure, modification, damage or destruction be it accidental or malicious.

[1] If found and held accountable for a security breach by a Court of Law or by the Information Commissioners Office, potentially both the individual and corporate entity may be subject to sanction.

Term	Description
Information Security Breach	An Information Security Incident where it is confirmed that a stated organisation policy or legal requirement regarding Information Security has been contravened.
Information Security Incident	Any event/information that warrants concern by Business Information Security that may also possibly affect Business Customer information systems, clients, or business partners.
Information System	Information in any media type, hardware, software, supporting networks, processes and human resources that support its acquisition, processing, storage and communication.
Secure	A term used in this document to define the requirement to manage information in a manner so as to minimise the risk of a Security Incident occurring through unauthorised disclosure or access to controlled information
The Business	MyTutor classified as Private Limited Business[2]
The Business Personnel	Includes all MyTutor's employees as well as all temporary staff, contractors, consultants and any third party with whom special arrangements have been made e.g. Confidentiality and Non-Disclosure Agreements.
CTO	Chief Technology Officer
Security Forum	MyTutor's forum where information security matters are discussed and activities related to information security are co-ordinated.
ICT	ICT, or information and communications technology

6. Duties and Responsibilities for Information Security

Role or Team	Description
Chief Executive Officer	Has overall accountability and responsibility for Information Security within MyTutor on a day-to-day basis the Information Security Lead will be the CEO as the Senior Information Risk Owner.
Senior Information Risk Owner (SIRO)/CTO	Will act as the advocate for information risk on the Business Board and in internal discussions, and will provide written advice to the Chief Executive on the content of their annual statement in regard to Information Risk.
Human Resources	Shall be responsible for ensuring that suitable contracts and non-disclosure agreements are in place with external contractors before access to MyTutor Information is given. These contracts require the contractor to comply with all appropriate security policies.
IT Systems and Data Manager	Is responsible for the implementation and enforcement of the Information Security Policy.
Line Managers	Are responsible for ensuring that all their staff (permanent and temporary) and contractors are aware of the Information Security Policy and that it is implemented fully in their area of responsibility.
Procurement	Shall be responsible for ensuring that suitable contracts with non-disclosure

Role or Team	Description
	clauses are in place before access to MyTutor's Information is given. These contracts shall ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.
Security Forum	Is responsible for ensuring that MyTutor complies with the Data Protection Act 2018 and as amended and that Information Governance standards are effectively managed and implemented.

7. Policy Review

This policy will provide a measure against which information security incidents can be assessed and subsequently managed.

MyTutor (via the Security Forum) will review this policy on an annual basis or in response to an actual or perceived increase in information security risk.

8. References

These references below are those most directly relevant.

#	Title	Description	Comment
1			This is likely to be updated so always check for the latest version
2			
3			
4			This is likely to be updated so always check for the latest version
5			
6	The Regulation Register	Current list of legislation relevant to MyTutor	This is likely to be updated so always check for the latest version

9. Document Control

9.1. Contributors, Reviewers, and Approvers

#	Role	Name	Comment
1	Approver	Bertie Hubbard CEO	
2	Content Author		
3	Reviewer	Michael Nuttall CTO	
4	Producer		

9.2. Document Maintenance

This section holds central information, it includes 'bookmarked' data which can then be reflected into other parts of the document.

#	Name	Variable	Description	Comment
1	Next Review Date	22/7/2021	The latest date by which this document needs to be reviewed	This document is intended to be reviewed annually by the Security Forum. It can be reviewed prior to date here. This will be set when the document is Released
2	Document Date	15Sep2020 15:31	The date for this version of the document. It uses the DM_Document_Date bookmark	For Approved versions this will usually use the {SAVEDATE} field code. Released versions will use a text string for the date
3	Expiry Date	ddMMyyyy	Date at which the document is marked for deletion	This would only be applied if decided at review.
4	Status			Currently uses DOCPROPERTY Status Custom field
5	Version Number			Currently uses DOCPROPERTY Version Custom field

9.3. Document Access Control Categories

The access categories/classifications in use

#	Category (Classification)	Circulation	Comment
1	CONTROLLED	Can only be circulated to The Business personnel, and selected approved business partners/third party suppliers	
2	The Business	MyTutor	The list for Read/write/edit is provisional and can be extended

9.4. Version Control

Version	Status	Actions	Action By	Date Started
0.1	Draft	Initial draft: replaced all previous information security polices		
1.0	Released	Reviewed and Amended for Final Release		
1.1	Released	Minor amendments		

9.5. Applied ISO27001 Controls

Control Ref	Title
A.7.2.2	Information security awareness, education and training
A.7.2.3	Disciplinary process
A.8.1.3	Acceptable use of assets
A.9.3.1	Use of secret authentication information
A.11.2.8	Unattended user equipment
A.11.2.9	Clear desk and clear screen policy
A.12.1.1	Documented operating procedures
A.12.5.1	Installation of software on operational systems
A.16.1.2	Reporting information security events
A.16.1.3	Reporting information security weaknesses