IT MOBILE EQUIPMENT SECURITY POLICY

Ref No	0036	**Version**	2.1
Dept	IT Services	**Last Updated**	June 2019
Responsible Manager	IT Manager	**Next Review**	June 2022
Date Approved	14.06.2019	**Category**	Public
Where Approved	Senior Leadership Team	**Covers**	Staff/Students

Contents

Scope 3
Introduction 3
Property 3
User Responsibility 3
Loss or Theft of Mobile Equipment 3
The installation of unlicensed or malicious software 4
Anti-Virus Software 4
Data Copyright Requirements 4
Data Protection 4
Care of Equipment 4
Security Requirements 5
Policy Review History 6

Scope

This policy applies to all Telford College staff and students using mobile equipment, such as but not limited to; notebook, Tablet, Mobile Phone, camera and laptop devices owned by the College. It defines the requirements to minimise the security risks associated with mobile equipment and ensures that the person allocated the equipment assumes the appropriate level of responsibility for its security.

Introduction

Mobile equipment is especially vulnerable to loss and theft. Opportunistic and organised thieves may target this type of equipment both within the College and when users are away from their "base" location. As well as stealing for financial gain there are a growing number of thefts specifically for the sensitive data the equipment may contain. Such information, if revealed, could cause embarrassment, loss of reputation or significant financial or commercial impact to the college.

Property

Mobile equipment issued to staff or students remain the property of Telford College. When equipment is allocated to a user, the user assumes temporary "custodianship" of the equipment. Upon allocation of the equipment, the user must complete a Mobile Equipment Custodian Agreement and undertake to comply with the Mobile Equipment Security Policy. By signing the agreement the user is accepting responsibility for the security of their mobile equipment and the information it contains. Equipment issued is for the sole use of the custodian during this period and must not be loaned out or used by a third party.

User Responsibility

The college will require the return of equipment if:

- An employee leaves the employment of the College
- A student is no longer an enrolled student of the College
- Requested to do so by his/her manager or tutor or any other senior manager of the College.

The equipment (and all peripherals) must be returned in good condition within one week of the due date of return. It must be returned to the user's manager or supervisor, and the original "Custodian Agreement" re-signed. Only after the resigning of this agreement is the individual released from their responsibility for the "custodianship" of the mobile equipment.

Loss or Theft of Mobile Equipment

If the equipment is lost or missing, believed stolen, the custodian must report the matter to the police. The police will issue a reference/crime number. This number must be reported to the IT User Portal Desk (extension 2284) immediately so that college's insurers may be informed. The custodian must provide a written report to IT Services detailing what they think may have happened and when and to whom the matter was reported.

Custodians with writing difficulties can get support writing up the loss/theft report from either the Learning Support Manager or IT Services.

The college reserves the right to claim the costs of replacement equipment from the custodian if the procedure set out in para.11 have not been followed. This may be in the form of a deduction from salary to cover the costs or invoice. In agreeing to the loan of this equipment the custodian is agreeing to this course of action.

The installation of unlicensed or malicious software

The use of unlicensed software (software privacy) is illegal and puts the College at significant risk of legal action. All software must be validated and approved by IT Service BEFORE being installed into the IT environment.

Unmanaged installations can compromise the devices operating environment and also constitute a security risk, including the unintentional spreading of software viruses and other malicious software.

Software MUST NOT BE installed by the custodian of the equipment. If it is proven that this has taken place then disciplinary action may be taken.

- You must not install software that you have purchased. All software for college owned equipment MUST be purchased by the college.
- Mobile equipment is for college related work only.

Anti-Virus Software

All mobile equipment at risk from malware must have the College standard anti-virus software installed. This ensures the college's information system and data are protected from the risk of virus infection. A process must be in place to ensure AV signatures are kept up-to-date if the equipment is to be used off-line (from the college network) for an extended period. Please see the College Anti-Virus policy for further information and user guide(s).

Data Copyright Requirements

Refer to policy

Data Protection

To ensure that sensitive information is secure, it must be stored on the College network servers which are automatically backed-up as a matter of course.

Mobile workers must ensure that when they are onsite; they turn on their mobile devices to ensure their data synchronises with college servers. This will happen automatically but can take a while dependant on the time away from site.

All mobile devices provided by the College are compliant with GDPR. Appropriate security configurations and encryptions and have been applied to the devices to secure the data held on them.

All IT base equipment is to be returned to IT Services one week before termination of employment by the college. This would include but not limited to mobile phones, cameras, laptops, tablets including memory sticks and or external hard drives, whether they be mechanical and or solid state-based devices. Failure to return these devices would be in breach of the Data Protection Act and GDPR Law for if there were any data pertaining on them that is either student and or staff based PII (Personal Identifiable Information). Telford College would also pursue reimbursement at market value for if the device/s were not returned to IT Services one week after termination of employment.

Care of Equipment

The custodian of the mobile equipment is responsible for its care. The following recommendations on care and maintenance should be followed:

- Be careful not to bump or drop the device, do not carry items with it that could harm it and do not put any objects on top of it. Cases, although strong, are not made to support additional weight.

- Take care when handling and storing the network connection cables. They can be easily damaged.
- When transporting mobile equipment always turn it off and put it in the carrying case.
- Avoid touching the screen of Laptops/netbooks etc. as the TFT screen is easily damaged.
- Avoid subjecting the device(s) to extreme temperature changes. Components can become very brittle and easy to break in cold temperatures and can melt or warp in high temperatures. As a general rule, the mobile equipment is safest at room temperature.
- Keep all liquids away from the device issued. Almost any liquid split on the device can result in extremely expensive repairs.
- Keep drives and the mobile devices away from magnetic fields. Magnetic fields can erase data on hard drives.
- Whenever possible, avoid turning off mobile equipment or other similar devices when the hard drive light is on because data on the hard drive could be lost or corrupted.
- Agree, when requested, to return your device(s) to IT Services for a health check. Failure to comply with this request will result in you IT account being disabled until IT Services complete the health check.
- USB Drives/Pens must comply with college Data Storage Policy; this means data should be encrypted.

Security Requirements

The custodian must take the following physical security preventative measures. Mobile equipment must not be:

- Left on view in an unattended vehicle, even for a short period of time.
- Left in a vehicle overnight.
- Positioned so that they are visible from outside a ground floor window, unless there is no alternative.
- Mobile equipment displaying sensitive information being used in a public place e.g. on a train, aircraft or bus, must whenever possible be positioned so the screen cannot be viewed by others.
- When leaving mobile equipment unattended for any extended period users must: Lock it away in a robust cabinet or alternatively lock the door of an individually occupied office.
- Store in a secure place in the users home.
- In vulnerable situations, e.g. public areas such as airport lounges, hotels and conference centres, mobile equipment must never be left unattended.
- Portable computers should whenever permitted be carried as hand luggage when travelling, preferably in bags sporting bright colours or large tags, as this will deter many potential thieves.
- Where any of the above rules are either inappropriate or impractical (e.g. staff/students on field trips) the custodian is responsible for taking all the reasonable steps to minimise the risk of loss or damage to mobile equipment.

Policy Review History

Version	Review Date	Reviewer	Reason for Review
V2	15/11/2019	IT Manager	Changes to data protection