Inspiring Futures Through Learning

Inspiring Futures Through Learning

Use of Personal Devices (ICT) Policy

April 2021 to April 2023

At Inspiring Futures through Learning, we are driven by our pursuit of excellence every day. We have high expectations of learning, behaviour and respect for every member of our community. We create independent, articulate thinkers and learners who have confidence in, not only their individual ambitions, but also those of the Academy and The Trust as a whole. We have collaboration at the heart of everything we do and our vision is to nurture exciting, innovative, outstanding Academies who embrace change and provide a world-class education for all it serves.

***Including all IFtL Schools, Milton Keynes Teaching School Alliance and Two Mile Ash Initial Teaching Training Partnership**

Policy name:		Use of Personal Devices (ICT) Policy
Version:		V2
Date relevant from:		April 2021
Date to be reviewed:		April 2023 *This policy will be reviewed every two years unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this Policy.*
Role of reviewer:		IFtL Head of Operations
Statutory (Y/N):		Y
Published on website*:		3C

Policy level:**	1
Relevant to:	All employees through all IFtL schools and departments
Bodies consulted:	
Approved by:	IFtL Finance and Resources Committee
Approval date:	29th June 2021

Key:

**** Publication on website:***

IFtL website		**School website**	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

***** Policy level:***

1. Trust wide:
   - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
     - *Approved by the IFtL Board of Trustees.*
2. Trust core values:
   - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore from the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
     - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*

3. School / department policies
   - These are defined independently by schools / departments as appropriate
     - *Approved by school / department governance bodies.*

Purpose

Modern ways of working often involve accessing data 'on the go' or outside of what may be regarded as normal working hours.
The majority of IFtL employees will have access to a work device to allow them to efficiently access the information that they require in order to carry out their work effectively. Some employees, however, may not have access to a work device.

Some employees may also wish to amalgamate data onto a single device, particularly with mobile phones, rather than carrying 2 devices. The use of BYOD in today's workplace is becoming more prevalent and some employees may have an expectation that certain aspects of their work, email for example, should be readily available on whatever device they choose to use.

The balance between allowing employees reasonable access to data on the move and ensuring that data is kept secure and adequately protected can be difficult to maintain.

In order to allow access to work data from personal devices, IFtL have produced this Use of Personal Devices Policy to ensure that appropriate steps are taken to ensure that our data is safeguarded if accessed on devices that are privately owned.

Scope and Applicability

This policy is applicable in all schools and academies within the IFTL MAT as well as within the IFTL offices, the MKTSA Teaching School and any other buildings within the control of IFTL.

Abbreviations & Definitions

BYOD – Bring Your Own Device
MDM – Mobile Device Management
VPN – Virtual Private Network

Use of Personal Devices

Should a staff member wish to access work data on a personal device, the following should be considered;

- Who has access to the device? (Consider employee's family members and what sort of information they might gain access to)
- Is the device password protected?
- Is the device encrypted?
- Does the device have anti-virus and anti-malware software?
- Is the device firewall enabled?
- Is the Wi-Fi connection that the device is connected to appropriately secure?
- What procedures are in place to ensure access is revoked if the employee leaves?

All organisations are legally bound to ensure that any company data, including email, is as secure on personal devices as it would be on a company server.

An appropriate procedure should be implemented by schools to enable an appropriate level of protection for data if staff are permitted to work on their own personal devices.

In all cases, where staff are using personal devices, they are bound by the same policies and procedures when using such devices as would be applied to staff that have been issued a work device.

Staff should wish to use personal devices for work, they should be aware that the trust or the school may require certain software to be installed on said personal devices (such as mobile device management software, anti-virus, anti-malware or encryption software) and will require that devices are kept up to date with updates and patches being applied as they are released.

Staff should also NEVER download and retain data on their personal devices. If documents need to be downloaded in order to work on them, they must be re-uploaded and deleted from the device as soon as they are finished with (this includes deleting the item from the recycle bin).
Ideally, documents should be worked on within the portal environment.

Remote Access and VPNs

Although issues with VPNs are not limited to access via personal devices, they are included within the scope of this policy for clarity.
Allowing personal devices to access networks via VPN introduces increased risks from virus and malware transmission as many personal devices may not have the same level of security as that of work issued devices.
Where schools permit access to the school network from outside the building via a VPN, they should ensure that appropriate security is in place to ensure that users can only access the areas that they are required to access.

Root access, or access to any of the administrative functions on the server, should never be available over a VPN and schools should work with IT support companies to ensure that this is the case.
Any passwords issued to allow access over a VPN should be unique to the individual and should not be shared under any circumstances. It is critical that there is full traceability of VPN access and all users must have their own access details.
The ideal solution is to disable all VPN access and to move all document storage to the portal.
The portal is a Microsoft Sharepoint hosted solution which is secure by design and designed to be accessed from anywhere with an internet connection.
Moving document storage to the portal removes any issues with VPN and remote access to servers.

Use of Mobile Phones or Tablets

Many staff use their mobile phones or tablet devices to access their email. Although this is standard practice, steps still need to be taken to ensure that this practice ensure that our data is adequately protected.

Mobile devices must always be protected by a PIN code or other appropriate security settings to ensure that unauthorised access is prohibited.
Always use official apps to access email. For example, iPhone users should use the Outlook app to access email rather than the native iPhone email client. This will allow Touch ID to be activated within the app so, even if the phone itself is unlocked, email cannot be accessed without providing the fingerprint again. Other phones may have similar security measures such as facial ID or PIN lock. These should always be used.

Schools should consider the use of MDM software such as Microsoft Intune or Impero. This would allow schools to retain some control over the apps and the data within them. Apps could be remotely locked or deleted, for example, if an employee were to leave their employment.
Intune is available as an add-on to the Trust's Office 365 licensing for a small annual charge per employee per year.

Use of Personal Laptops

Use of personal laptops for work should be avoided wherever possible. When staff have no option but to use their own devices, the following should be considered;

If staff are working on a personal laptop or desktop PC, a separate account should be set up for work. This account should be password protected and no other person, including family members, should be allowed access to this account.

Laptops or desktops should have anti-virus and anti-malware installed. If they do not have this, the school may need to supply this and ensure that it is installed and configured correctly.

Hard drives, particularly for laptops, should be encrypted. If Windows 10 is in use, this is a built-in feature with some versions and just needs to be activated.

The ‘end of life’ procedure for devices should be assessed. It is critical that hard drives are securely erased or destroyed prior to any devices that have held sensitive data being sold or otherwise disposed of.

This is not an exhaustive list of measures and your IT department should be consulted to ensure that all necessary steps have been taken to ensure that devices are adequately secure.

The ideal scenario is to ensure that all staff that need access to a work device, have access to a work device so that use of personal devices is not required.

General Access to Work Systems

Staff may routinely access email, the portal or other hosted systems via a web browser or an app from any personal device.
Although this is acceptable, staff should regularly be reminded of the need to keep data secure, to sign out of all systems once they have completed what they are doing, to not store passwords if a device is shared with anyone, even if that person is a colleague or a family member and of the importance of data security.
It is recommended that this is a standing item on the agenda for inset meetings.

Employee Wellbeing and Work-Life Balance

It is important that wellbeing and an appropriate work-life balance are considered when discussing the use of personal devices with employees.
Staff should be able to switch off from work outside of their contracted working hours and allowing access to work data from personal devices may make this more difficult.
Staff should be made aware of how to exit apps or how to switch off notifications when necessary.