Home Working and IT Policy

- All requests for remote/mobile computer working must be formally authorised by the Chief Executive Officer
- No Education Fellowship owned computer equipment should be taken off site without written authorisation from the appropriate Director.
- All users of remote mobile computing devices must understand their responsibility to prevent theft and protect data.
- No unauthorised software may be added to The Education Fellowship owned computer equipment nor any copies taken of the software on the computer hard disk. Software licensing requirements must be complied with
- All remote/mobile computer devices and their owners must be recorded on an asset register. Staff who work in either a mobile or remote manner must be provided with specific guidance on the requirements incumbent upon them to protect equipment and information and must sign a declaration to confirm that they have received such guidance
- When working at home on a privately owned computer with Internet access via an Internet Service Provider, access to the organisation will be via Office 365 giving access to data files and the email services. Any Education Fellowship business must be done using this connection and organisation work must not be stored on the home computer's hard drive or directories unless encrypted and/or password protected and stored within a secure and protected area of the home computer's memory
- Home workers connecting to The Education Fellowship Office 365 systems must ensure that appropriate security measures are taken to protect computers and networks from unauthorised access by taking the following actions:-
    - Users of the organisation's network should keep usernames and passwords secure to reduce security risk if the computer is stolen.
    - No person other than the authorised user is permitted to access the device and data files.
    - Where home computer equipment is provided by the user, they must ensure that access to portable computer equipment requires individual user accounts and passwords

- The current version of this policy is held on The Education Fellowship's Document Management System (DMS). Check that this printed copy is the latest issue
- Users must not disclose their password to anyone else.
- Users must not use the organisation's computer equipment for unauthorised activities
- Users must not use the organisation's computer equipment in any way that contravenes current legislation
- Users must not attempt to access data or information not normally made available to the user or required by them for the purposes of their work
- Users must follow procedures in place for the protection of The Education Fellowship's equipment from the effects from computer viruses. To restrict the possibility of viruses being transmitted to the organisation's computer and network users must not use their own personal computer for work related activities unless appropriate and up to date anti-virus and malware scanning software and a firewall has been installed and is running
- If files are saved onto an external hard drive, CD or memory stick they must be scanned for possible viruses and data encrypted and/or password protected. Information temporarily stored on portable media should be deleted as soon as possible when no longer required
- Prior authorisation to remove data files is required. Data files should only be removed offsite when absolutely necessary. All staff who work with person identifiable data at home must obtain formal authorisation by their line manager before the data files can be taken offsite. A log must be kept of the files removed and when returned to the office
- Data must only be used in accordance with the legitimate business of the organisation. When computer equipment and data is removed from The Education Fellowship premises, it is the responsibility of the member of staff to ensure its safe transport, appropriate use, storage and return. Mobile equipment should not be left unattended at any time or left in a car overnight and should be kept out of sight when being transported in a vehicle. IT equipment must be transported in a secure and clean environment. The organisation's equipment is not insured, unless it is in a lease car provided by the Trust, and the staff members may be liable for the loss if reasonable precautions are not taken. If the vehicle is an Education Fellowship provided lease car, the insurance will cover the equipment whilst they are in vehicles. It is the responsibility of the staff using the equipment to ensure that computers are not left visible in unattended vehicles

- Reasonable steps to minimise visibility of computer equipment from outside the home must be taken and to secure windows and doors when the home is unoccupied. Any confidential documents taken home must be stored securely at all times
- Any theft, loss of computer equipment or damage or misuse of data must be reported to the appropriate Director without delay in order to maintain the asset register. Failure to do so could incur disciplinary action
- The organisation has an email policy that must be followed. However the following points apply directly to staff working from home and using their personal email account. Person identifiable data must not be used in any communications sent by email. Internet email services of any sort are not secure and should not be used to send person identifiable or other confidential information
- Staff must not automatically forward their email via a commercial internet service provider such as Hotmail, Google etc. Staff sending emails should be aware that it is not suited for confidential communications. Various systems are used for receiving email and there is no guarantee that the addressee will be the only person to see the email and it is possible that the communications sent by email could be lost, accessed or modified by unauthorised individuals
- It is the responsibility of the home worker to ensure that they comply with the Display Screen Equipment Regulations regarding the use of video display units when they use the PCs or laptops as a significant part of their normal work and staff must follow the HSE recommended guidance for posture and breaks
- Members of staff using smartphones or tablets such as iPads must contact the IT Department to ensure that they are suitably configured and protected from theft or loss of data. The IT Department must ensure that procedures exist to allow only authorised devices to connect to and download information from or synchronise with the organisation's networks and PCs. Users must ensure that devices require password or PIN authentication to access and have time outs and must ensure that data is encrypted
- The IT Department will configure devices to protect data and provide for adequate authentication before connection and must ensure that they only allow authorised mobile email devices to receive corporate email and must ensure that their email devices require password or PIN authentication to access and have time outs and must ensure that email device data is encrypted