Remote Working Policy

Approved by TCES Operational Board on behalf of

Thomas Keaney, CEO and Schools' Proprietor

Date of next formal review, Sept 2024

This policy applies to the TCES National Online School

Contents

Introduction

This policy applies to those staff members employed by TCES Online National School. This policy applies to remote working, whether by an employee who spends all of their working week at home ("a permanent remote worker"), part of their working week at home ("a part week remote worker") or only works at home on an occasional basis ("occasional remote worker"). The term "remote worker" or "remote working" in this policy covers any of these employees.

The Company supports remote working due to the nature of our online service. All employees will be required to sign our TCES 'Remote Worker Agreement'. Employees signing this agreement must comply with its contents. Where an employee has worked from home from the commencement of their employment or before the publication of this policy, all terms will be as previously defined, usually within their contract of employment. A Remote Worker Agreement must be completed to reflect existing arrangements, with updates as necessary under the requirements of this policy.

General Principles

Those affected by this policy are TCES National Online School employees who provide a service to this service and TCES Schools.

TCES wishes to accommodate working location preferences where it helps the efficiency and effectiveness of the staff member.

The remote working environment

Employees should ensure that they have a suitable environment in which they can focus on work, free from disruption e.g., by having adequate care arrangements in place for dependents who may be at home during working hours. Remote working must not be used as a replacement for a dependent's care arrangements except in exceptional circumstances in agreement with the line manager and as reflected in the Family Friendly Policy.

The environment must also be safe and comfortable and fulfil all Health & Safety requirements (see below).

Working arrangements for remote workers

Working from home will only be possible if it can be ensured that their home conditions are conducive to effective working.

Staff members working remotely must ensure that they are readily available when colleagues and stakeholders would expect to reach them during the working day, are able to receive calls and/ or attend virtual meetings throughout the working day when not teaching.

For insurance and safety reasons remote workers must not hold meetings with clients, colleagues or any non-Company persons in person at their home unless otherwise

authorised/requested by the Company for legitimate business reasons. Where meetings are required, these should take place on Company premises wherever possible, or in an alternative and suitable meeting space.

Video/conference calls should be considered to be an alternative suitable option. In these instances, remote workers must adhere to the TCES dress code, and must ensure their on-screen background depicts a professional setting, using background filters if required. Where meetings take place via video/ conference calls, remote workers must ensure that they can hold the call with minimal disturbances, that confidential information is not overheard, and safeguarding is adhered to. As with

MS Teams meetings, it us usual practice for cameras to be on.

Home address and other personal details must not be disclosed to students or their families.

Restricted access materials must not be taken out of your home, copied, or compromised in any way and GDPR must be complied with. Remote workers must take precautions to secure sensitive information, including not printing sensitive information on home computers.

Standard working hours apply regardless of the employee's place of work and therefore apply regardless of remote working arrangements. These are contained in an individual's contract of employment.

Equipment

TCES will provide any necessary equipment as appropriate to a remote working role. This includes a staff laptop and pay as you go mobile phone. Mobile phones will have designated credit assigned, this can be topped up when required.

TCES will provide a Skyguard personal alarm device where required.

This excludes contributions to utility and Wi-Fi bills, printers, furniture, fixtures and fittings.

The following will apply to any equipment provided:

- it remains the property of the Company
- it must not be removed from the designated remote worker's address without the authority of Management
- it must not be used other than for work purposes unless otherwise agreed
- the remote worker is responsible for taking reasonable care of the equipment
- the remote worker will be responsible for any damage to equipment which goes beyond normal wear and tear, including the damage caused when transporting the equipment
- the remote worker must report any damage to or malfunction of the equipment, to Management as soon as possible

The remote worker should ensure that there is a strong and consistent internet connection available in order to support the work they are to carry out. Where there are connection issues affecting the remote worker's ability to carry out their duties, they must contact Management immediately.

Remote workers may be required to work from an alternative location, permanently or until the issue is resolved.

Remote workers will be required to sign a deduction from pay agreement for any equipment provided.

Workers may be requested to allow other employees of the Company, or contractors acting on the Company's behalf, to have access to their home, in order that those employees or contractors may:

- install, inspect, replace, service, repair or maintain Company equipment
- carry out a risk assessment
- collect items belonging to the Company on termination of employment, if they have not already been returned within the period requested

Insurance

All Company property provided to remote workers for use in their home will be covered under the Company insurance policy.

Any remote worker provided with Company property must not cause or permit any act or omission which will avoid coverage under the Company insurance policy. If in any doubt as to whether a particular act or omission will have this effect, the remote worker should consult Management immediately.

Remote workers who hold a household/home insurance policy should notify their insurer of their remote working arrangements and are responsible for ensuring that those arrangements do not breach any policy condition, restrictive covenant affecting their home address, local authority planning restriction or mortgage condition.

General liability

Remote workers remain responsible for ensuring:

- the safety of any visitors to their home, as well as any other family members, particularly children
- that the general fabric of their home and its fixtures and fittings, including in any area in which they work, are maintained in a safe and functional state for performance of work, including any parts of a domestic electric system
- that the costs of electricity, water, heating, telephone, internet connection and other utilities are paid

Confidentiality, data protection and use of Company systems

Remote workers must comply with the duties and obligations to confidentiality, data protection and use of the Company's systems and network under the Company's relevant policies.

In accordance with the Company's policies and procedures, remote workers are responsible for maintaining the security and confidentiality of any business-related resources, equipment, or information to which they have access, and in particular to follow the Company's IT Policy.

Remote workers should:

- take reasonable steps to restrict the access of family and friends to work equipment, materials, documents, or other data to avoid damage or loss and maintain business confidentiality
- unless essential, confidential paperwork should not be removed from your area of work, and in rare instances where it is necessary to work remotely with confidential paperwork, it should be stored securely when not in use
- ensure that all confidential material, paper or electronic, should be securely destroyed as soon as any need for its retention has passed
- take reasonable care of work-related information and Company property when travelling
- not install or update any software on to Company owned IT equipment without permission from Management
- not change the configuration of any Company owned devices
- allow the installation and maintenance of Anti-Virus software and any operating system updates when required
- not alter or disable any element of the configuration of devices or 'jail break' (modify to remove restrictions imposed by the manufacturer or operator) them
- only save business critical data in approved storage locations
- report all faults, stolen or lost hardware to Management
- ensure requests for upgrades of hardware or software are approved by Management prior to request; this includes mobile apps from the relevant provider
- in the event of a lost or stolen mobile device, report the incident to Management immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than the Company. If the device is recovered, it can be submitted to Management for re-provisioning. The remote wipe may destroy all data on the device, whether it is related to Company business or otherwise
- co-operate fully with any software or hardware audit conducted by the Company. The Company may be required to remove any equipment at the time of the audit for further inspection
- maintain security of and do not share any information concerning passwords, usernames, network credentials or requirements used to access the Company information and systems by remote working/mobile working with other employees, unauthorised users, third party vendors, family, friends, or members of the public

- always be aware of the potential for other people (including family, friends, and colleagues) to overlook screens and keyboards and view personal or confidential information, or passwords, and ensure this is not taking place
- be aware of surroundings and ensure work is conducted in a location where it is not possible for a screen/document to be seen or a conversation overheard
- ensure that all applications are properly closed/logged off, browsers are closed, and internet sessions are logged off, prior to network connections being logged off and closed
- send any email communications that have personal or commercially sensitive information using password protection/encryption where applicable (please see the TCES GDPR and Data Protection Policy for more information)
- Only use company supplied IT accounts to send any work-related email communications
- not install any screen savers on Company owned equipment
- when leaving desks temporarily during the working day, even if only for a few minutes for example during a break, lock all portable computer devices
- report any information or data breach or accidental disclosure immediately to Management
- not use hardware such as mobile phones, laptop, and tablets, not provided by the Company for Company business unless prior authority has been obtained from Management
- only use location-based services and mobile check-in services which use GPS capabilities to share real time user location with external parties when carrying out work duties

Access to Company data will be controlled through secure server access provided by the Company. This may include multi-factor authentication where applicable.

The Company will deploy updated Anti-Virus signatures and critical security updates to all users who work away from the Company premises. Remote workers must ensure that any Company devices are connected to the corporate network at least once every working week to enable these updates to install.

Health and safety risk assessments

The Company has certain obligations under health and safety legislation which may require it on occasion to perform a risk assessment of the work activities carried out by a remote worker. The purpose of completing a risk assessment is to identify the hazards relating to the remote worker's work activities and to decide whether sufficient steps have been taken to prevent harm to the remote worker or anyone else who may be affected by their work.

Risk assessments in relation to the working environment of a remote worker may, depending on what approach is viewed as most appropriate by the Company, be carried out by the remote worker, another employee or contractor on the Company's behalf (and to facilitate this the remote worker may be required to provide access to

their home to the extent described above), or as a self-assessment by the remote worker.

Where self-assessments are required, appropriate guidance and advice will be provided to the remote worker, and the remote worker is expected to cooperate fully and follow such guidance.

All risk assessment findings will be recorded and reviewed as appropriate.

For permanent remote workers, it may also be appropriate to conduct a Stress Risk Assessment to ensure the wellbeing and mental health of remote workers is well managed.

Display Screen Equipment (DSE) assessments

Display Screen Equipment (DSE) is a device or equipment with a display screen and often refers to a computer screen. However, it includes both conventional display screens and those used in emerging technologies such as laptops, touch screens and other similar devices.

In a work environment, desktop computers are traditionally looked at when considering DSE, but it is important to consider other display screens such as tablets, laptops, and smartphones.

The DSE regulations require an assessment/analysis of DSE so that the risks can be identified and controlled.

DSE assessments are required by all 'users' of display screen equipment. A 'user' is described as someone "who habitually uses display screen equipment as a significant part of their normal work". DSE regulations cover equipment such as the desk, screen, chair, disk drive, telephone, printer, document holder, work surface or other peripherals to the display screen equipment, and the immediate environment surrounding the equipment as well as the tasks being undertaken by the user of the equipment.

When using DSE, users should plan their activities so that their daily work is periodically interrupted by breaks, or changes of activity to reduce their workload at that equipment. To achieve this, users must ensure they take regular breaks during the workday for activity changes, for example phone calls, meetings, natural breaks, refreshments, or changes to posture to avoid stiffness, eyestrain and upper limb disorders.

Workstations should meet certain requirements however this is not always possible or suitable for some environments or tasks. Where this is not possible to do, the Company shall reduce the risks identified in consequence of an assessment to the lowest extent reasonably practicable.

Where a remote worker works with DSE:

- the Company will ensure a DSE assessment is carried out, that the equipment is safe and fit for use, and advice will be provided to the remote worker on how to use it safely, including information on breaks from work
- the Company will provide training on the set-up and use of DSE
- they may be entitled to eye tests paid for by the Company, in line with standard guidelines for other employees and in line with Company policy

In the event an accident occurs, or the remote worker contracts an illness or sustains an injury, or generally feels unfit to work, Management must be notified as soon as possible. A remote worker must also inform Management as soon as possible if they become pregnant.

For further health and safety information, see the Company's **Health and Safety Policy**.

Communication and meetings

To minimise the potential isolation of remote workers, and/or to allow for their proper supervision and management, Management will, where appropriate, involve remote workers in regular meetings. Remote workers are required to attend such meetings. If a remote worker cannot attend a scheduled meeting for good reason, they should notify the person organising the meeting in advance. If a remote worker does not attend meetings repeatedly, this may constitute a failure to follow a reasonable management instruction and may result in disciplinary action.

In addition to regular meetings, Management will ensure that regular contact is made between the remote worker and members of their team.

Remote workers may be required to attend Company offices and/or other locations according to the needs of the business.

Remote workers are expected to be contactable during the agreed hours of work. Contact outside these hours will only be made in cases of emergency.

Training and development

Training of remote workers will take place as appropriate and required. Remote workers will be expected to participate in any departmental or general training sessions, at Company premises where required.

Remote workers will have the same opportunities as office-based employees to apply for advertised vacancies within the Company.

Absence from work

Where a remote worker is unwell or unable to work, the normal absence and related reporting procedures available on the Company Intranet apply.

Monitoring and Review

The success of remote working depends on there being the necessary monitoring and support systems in place.

Although remote workers will not be treated any differently to office-based employees, different techniques may be required to manage remote workers. It is the responsibility of Management to have in place a system of monitoring by results, targets and objectives that are agreed with the remote worker so that output can be measured, and performance properly evaluated.

Remote working permission will be reviewed and possibly withdrawn, on a permanent or temporary basis, if it is demonstrated that:

- the performance of remote worker suffers as a result
- that the effective and efficient operation of the team or department is compromised
- that the ability of the wider organisation to fulfil its objectives is compromised