Zest Academy Trust

Working at home policy

Approved by Trust Board: 31 July 2018
Review Period: Biennial
Policy Date Last Reviewed: 07/01/2020
Person Responsible: CEO
Version Number: 2

Zest Academy Trust, Waterloo Road, Blackpool, FY4 3AG
T 01253 315370 **E** admin@zestacademytrust.co.uk **W** www.zestacademytrust.co.uk

CEO Mark Hamblett

Introduction

This policy has been created to give guidance to staff who work off site on Trust/Academy business. The policy provides staff with flexibility whilst maintain security and confidentiality.

The Trust expect staff to normally work within their workplace, however we recognise that there are times when working off site is necessary and mutually beneficial.

Definitions

Occasionally working from home
Occasional working from home means the employee performing specific work obligations required under their contract of employment from their home on an irregular basis.

Personal data
Personal data is information relating to an individual where they can be identified directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to an individual.

Responsibility

Whilst occasionally working from home it is the responsibility of the employee to work within the Trust guidelines and policies in ensuring current legislation is not breached.

The Trust provides filtered access to all employees and students through their personal accounts, whilst in school. Employees should take extra care when using the academy IT equipment to browse the internet whilst working at home.

Requesting to work at home

All employees wishing to occasionally work from home must secure the agreement from the Principal/CEO. The request should outline the proposed date and work which will be undertaken.

There has to be a clear business need identified for the employee to work from home. Examples could include completing a specific piece of work, which can be achieved more efficiently without the day to day interruptions.

Approving a request to work at home

When approving an occasional request to work from home the Principal/CEO must consider the following:

- The nature of the work being undertaken
- The nature of the employee's job role
- The impact on other employees
- The equipment required to work at home

Nature of the work being undertaken

The nature of the work must clearly be identified, for example:

- Budget setting, report writing, policy creation and other similar documents
- Marking and assessment
- Preparation and planning

If the nature of the work involves taking personal sensitive information off site then a risk assessment should be completed. The employee must ensure that the risk assessment is completed and authorised by the Data Protection Officer (DPO) before they take information off site.

Communication

Good communication is an essential part of working from home and off-site. Arrangements should be in place where employees should always provide their contact details to a designated member of staff with a contact telephone number that they are available to receive calls on during normal working hours for any necessary work matters. It is good practice to regularly check work emails.

Equipment and Security

Equipment needed to undertake occasional work from home will be IT equipment, internet and on occasions a telephone. The Trust will not provide IT equipment to employees unless it is part of their job role. Furthermore, it is the responsibility of the employee to ensure that they have insurance in place should the Trust property be stolen or damaged.

When working from home, the employee must be aware of the increased risk of a security breach. The employee must ensure that all documentation is stored securely and that any laptop or iPad is password protected and turned off when not in use. If a security breach occurs then the employee must refer to the data breach policy and report the breach immediately.

Employees are not permitted to store any personal data relating to the trust on their personal devices and should take note of the good working practices guidance in appendix A.

Health and safety

As most of the work being undertaken is administrative, low risk and undertaken on an occasional basis, the employee will not be classed as a 'homeworker'. However, to ensure safe systems of work, employees are advised to refer to the academy's ICT policy and complete the Health and Safety Executive, display screen equipment workstation checklist.

Guidance is issued to employees working from home to remind them of general risk assessment principles, to raise their awareness of potential risks to health and safety which may result from working at home and indicating possible action that can be taken to create safe working conditions and the right working environment.

Employees should also consider the following:

- Taking regular breaks from working at your device – a few minutes at least once an hour, stand up stretch and move around
- Keep your mouse and keyboard at the same level
- Check you seating position, do not slouch, make sure your lower back is supported
- Avoid bending or angling your wrists while typing or using a mouse

Monitoring

The Trust will monitor the effectiveness of all policies and procedures.

Related policies
The following policies are related to this data protection policy:

- data retention policy
- data protection policy
- data breach policy
- acceptable use policy

These policies are also designed to protect persona data and can be found at www.zestacademytrust.co.uk

Appendix A – Good working practices

Whilst working away from the Trust, especially when employees are using a remote connection, employees are reminded that they should be equally vigilant when accessing the files and folders located on the Trust's servers.

Whilst occasionally working from home, employees should still adhere to the Trusts acceptable use policy regarding internet access, this will protect employees, and the Trust from potential malware/virus issues.

- When working from home, the employee must be aware of the increased risk of a security breach. The employee must ensure that all documentation is stored securely and that any laptop or PC is password protected and turned off when not in use.
- Activity that threatens the integrity of the Trust systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- The Trust will not normally provide IT or other equipment, for example PCs, for an individual's use at home or at other locations.
- Under no circumstance are users allowed to download any software or obscene material using the internet.