ELATT Home-Working Policy and Guidance

Issue Date: 18.03.2020

Summary

DO:

- Use devices with adequate protection: antivirus and enable updated Windows defender
- Use Office 365 or VPN for all work involving sensitive and personal data
- Keep your device locked away and secure
- Work at home
- Follow ELATT's Data Protection Policies
- Only take documents home that have been pre-agreed with your manager, and keep them updated of progress
- Delete anything you have downloaded and worked on after every session
- Lock away all paper documents securely after you have finished using them.

DON'T

- Save work on desktops, local drives or portable data storage e.g. USB sticks
- Use unsecured public Wi-Fi e.g. in cafes or on public transport
- Work where other unauthorised people can see your files e.g. over your shoulder or in plain view
- Carry your paper files or devices on public transport unless pre-agreed and absolutely necessary. In this situation, pre-agree a data-moving strategy with your manager

Scope and definitions

1.1. This policy applies to all staff who use or access ELATT systems or information remotely either occasionally or as part of their contract. It applies to information in all formats, including manual records and electronic data.

1.2. 'Home working' and 'Remote working' means working outside of ELATT offices or outside of the secure ELATT computing environment; this includes working while connected to ELATT's WiFi networks.

1.3. 'Staff' includes anyone working on behalf of the ELATT or given access to ELATT data, eg visitors, students and subcontractors.

Purpose

1.4. To ensure that staff are aware of their individual responsibilities around information security when working remotely.

1.5. To ensure staff work in accordance with the ELATT's data protection policies https://resources.elatt.org.uk/elatt-handbook/8-data-protection/elatt-data-protection-policy-records-management.pdf

1.6. To provide policy and guidance for staff on secure remote working and so minimise the risk of unauthorised access to, and loss of, data.

1.7. Staff working remotely must ensure that they work in a secure and authorised manner as set out in the Key principles below.

Background and risks

1.8. Remote working presents both significant risks and benefits for ELATT.

1.9. Staff may have remote access to information held on secure ELATT servers, but without the physical protections available on-site and the network protections provided by firewalls and access controls there are much greater risks of unauthorised access to, and loss or destruction of, data. There are also greater risks posed by information 'in transit'.

1.10. The risks posed by remote working ELATT information can be summarised under three headings:

1.10.1. reputational: the loss of trust or damage to ELATT's relationship with its customers, partners or funders;

1.10.2. personal: unauthorised loss of, or access to, data could expose staff or students to identity theft, fraud or significant distress; and

1.10.3. monetary: some regulators, can impose penalties of up to £500k.

1.11. This policy sets out policy and guidance on how staff can work remotely in a secure and low risk fashion.

Roles and responsibilities

1.12. Any member of staff working remotely is responsible for ensuring that they work securely and protect both information and ELATT-owned equipment from loss, damage or unauthorised access.

1.13. Line managers are responsible for supporting their staff's adherence with this policy.

1.14. Failure to comply with ELATT information compliance policies may result in disciplinary action.

Key Principles

2. All staff must comply with these principles when working remotely.

2.1. Do not use IT equipment or paper documents where it can be overlooked by unauthorised persons and do not leave it unattended in public places.

2.2. Use automatic lock outs when IT equipment is left unattended.

2.3. Ensure that if the master copy of the record, whether paper or electronic, is removed from ELATT premises, administration team and line manager are aware. Master copies must returned as soon as practically possible.

2.4. Transporting devices and paperwork on public transportation must be kept to a minimum and should be using a lockable case or another secure method. All plans to transport data should be discussed with your line manager.

2.5. IT equipment must have anti-virus software or at the very least have the updated version of Windows defender (Other operating systems equivalent)

2.6. It is the responsibility of the member of staff to ensure that the working environment and space is safe and suitable for remote working.

2.7. Do not use public Wi-Fi or non-ELATT authorised ways of working or remote working products, like gotomypc or using internet cafes, when accessing ELATT systems and data. VPN is the ELATT authorised way of working remotely and any exceptions must be authorised by ELATT.

2.8. Access to certain systems and services by those working remotely may be deliberately restricted or may require additional authentication methods. Any attempt to bypass these restrictions may lead to disciplinary action.

2.9. Staff should be authorised to remotely access ELATT information or systems by an appropriate authority, usually their line manager (or equivalent).

2.10. A risk assessment should be conducted before the remote working begins.

2.11. If ELATT provides IT equipment to staff, it will supply devices which are appropriately configured to ensure that they are as effectively managed as devices in the secure office environment. Unlike personally-owned devices which are managed by their owners, ELATT-owned devices will be managed by Tech Support. Staff who have been provided with ELATT-owned IT equipment to work remotely must:

a. only use this equipment for legitimate ELATT purposes;

b. not modify it unless authorised by Tech Support;

c. return the equipment at the end of the remote working arrangement or prior

to the recipient leaving ELATT; and

d. not allow non-staff members (including family and friends) to use the equipment.

2.12. Users who process ELATT-held information on privately-owned equipment are responsible for the security of the device and must follow ELATT's policies

2.13. Staff working remotely must ensure that information is retrievable. Freedom of information and data Protection gives the public rights of access to information held by ELATT, and this covers information held remotely, on paper and electronically. In the event of a request for information staff must retrieve *all* relevant requested information, whether held remotely or at ELATT, and within a reasonable time so that the ELATT can meet the relevant statutory deadlines for responding.

2.14. Staff working remotely must adhere to the ELATT's Data Protection Policies, and in particular ensure that information held remotely is managed according to respective ELATT records retention plans and securely deleted or destroyed once it is no longer necessary to process it remotely. This includes any downloads made from Sharepoint to your device.

2.15. Tech Support will need to check the licensing provision for dedicated or specialist software to ensure that it covers remote working, including in the country or region where remote working is to be performed. Please get in touch with the team if you have any specialist software.

2.16. **All staff, students and others who work on behalf ELATT must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any ELATT-owned IT equipment or data- electronic of paper based) immediately to your line manager, in order that appropriate steps may be taken quickly to protect ELATT data.** Failure to do so immediately may seriously compromise ELATT security and, for staff, may lead to investigation and potentially action under the disciplinary procedures.

Home-working risk assessment and policy agreement

As outlined in the policy, any ELATT staff working from home is likely to be handling sensitive data, which includes students' personal details. Below is an assessment for staff working from home, which must be completed and signed, and returned to your manager by email/paper copy.

Risk	Yes/No	Action
Are you only accessing the information via a VPN or via Microsoft 365 (encrypted)?		
Is there low risk of theft? (At home all day? Kept in secure room when not in use?)		
Can other people see your screen or data on paper documents? (Over your shoulder or through a window)		
Will you be storing any data on the local drive of the device?		
If you need to repair your device, is the company that you use subject to a contractual agreement which guarantees the secure handling of any data held on the device?		
Have you assessed the health and safety risks of remote working? E.g. desk height, room under your desk for feet, wire trip hazard, regular rests, monitor height		

I confirm I have read and understood ELATT's home-working policy and have completed a risk assessment for home-working.

Name:

Date: