Homeworking – Best Practice Guidelines

Based on a template from Information Governance (IG) Services (Dudley).

Home Working Best Practice Guidelines

Introduction

The COVID-19 crisis has changed the way we live our lives and do our jobs. Keeping social distancing rules means many trust staff are working from home for part of the time and adapting to new ways of doing their jobs.

When working from home staff may be taking all kinds of information out of the Trust to the home setting. This could involve taking pupil books home to mark, completing lesson plans, or logging into the Trust network to catch up on emails, video conferencing, etc. When working at home, staff may also need access to records held electronically.

It is recognised that technology can also help us to stay connected and there are various video conferencing software and apps to help Trusts hold staff meetings, conference calls, and generally keep in touch! The Trust uses Google for Education as a platform for communication.

When working from home there are other considerations including network security and privacy issues.

This guidance document provides staff with best practice guidelines on areas to consider to ensure they are compliant with the requirements of data protection law and not putting themselves or the Trust at any risk.

It must be remembered that Data Protection Act 2018 applies to those who are working at home and using mobile devices or video conferencing facilities just as it does to those who are working within a Trust building.

What are some of the risks?

Article 5 (1)(f) of the UK General Data Protection Regulation requires that personal data should be:

'*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).*

Article 4 (1) of the UK General Data Protection Regulation defines personal data as:

'any information relating to an identified or identifiable natural person ('data subject'): an identifiable natural person is one who 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'.

The Trust needs to consider the value of Home Working for members of staff against the risks. For example:

- Loss/Theft of equipment or data
- Loss/Theft of Manual files (although Trust policy is that not manual files are to be removed from Trust property)

The main issue when working at home is that it presents security problems. For example:

- The journey home introduces a risk of loss or theft whilst in transit.

- The average home is very easy to burgle or it may be unoccupied part of the time which could result in the theft of equipment or information e.g.chromebooks, (note, not memory sticks as Trust policy forbids staff from using them)

- Family members or visitors to the home may gain access to Trust equipment or information

In nearly every case, it will be more important to protect the information rather than the equipment.

This guidance goes onto highlight some of the key risks of home working, identifying what the issues are and the mitigating actions as follows:

- **ISSUE:** Connectivity

RISK: The network staff may be using is not secure
MITIGATING ACTION: When accessing personal data consider the security of the network. Ensure that the data security settings have been appropriately set on your home router. If in doubt, tether to your work mobile phone as two factor remote access is in place.

- **ISSUE:** Phishing

RISK: Data security breach
MITIGATING ACTION: Staff being aware of their responsibility as the last line of defence to ensure the integrity and confidentiality of the Trusts IT infrastructure. Staff verifying with colleagues that a message is genuine, before clicking on any links. Staff to complete training provided by the National Cyber Security Centre.

- **ISSUE:** Use of personal devices

RISK: The risk for a data security breach is greatly heightened if staff use their personal devices for Trust business
MITIGATING ACTION: The risk of a data breach is greatly reduced when staff use work devices for work activities and personal activities are restricted to employee owned devices. This is explicit in Trust policy.

- **ISSUE:** Security of Privacy

RISK: Home working can mean that documents may be seen and work related conversations may be overheard by others
MITIGATING ACTION:. Staff need to understand the risks associated with the data they are handling and ensure there is privacy when working. Training will be provided for staff

- **ISSUE:** Screen sharing

RISK: Unauthorised access to personal data
MITIGATING ACTIONS: Staff need to be aware of their surroundings when screen sharing. This may include images of their screen of personal data being reflected from glass such as mirrors and windows. Staff to be provided with training

- **ISSUE:** Training

RISK: Staff are unaware of the risks in terms of remote home working
MITIGATING ACTIONS: Staff will need to be aware and understand the risks that are under their control when remote home working. Training and updates to be provided.

- **ISSUE:** Video Conferencing

RISK: Unauthorised access to personal data
MITIGATING ACTION: Staff need to be aware of their surroundings when video conferencing. This may include images of their screen of personal data being reflected from glass such as mirrors and windows. All staff are aware of risk assessments and requirements, and pupils have a 'code of conduct' for accessing live lessons e.g. they must be dressed appropriately and not in their bedrooms.

Consequences

Any information relating to an individual i.e. pupil, parent, member of staff, that is lost, stolen or disclosed to an unauthorised person has to be treated as an information security incident.
Staff must notify the Academy Data Protection Officer immediately of any loss or suspicion of loss of any confidential information or inappropriate disclosure to ensure that appropriate action is taken to investigate and manage such incidents.

The consequences of this incident will vary based on the nature of the information which has been lost / stolen. There may be safeguarding implications i.e. if it is a looked after child; alert your Academy's Designated Safeguarding Lead immediately if this is the case.

A serious loss of sensitive personal data may lead to a monetary penalty or Information Commissioner investigation that could damage the reputation of the Trust.

As well as the Trust, individual members of staff can also face action under Data Protection Law or face disciplinary action if found to be in breach of policy. The UK General Data Protection Regulation allows individuals to seek redress through civil routes and claim compensation for any harm caused by a data loss. You could even be committing an offence by sharing information with other members of staff who do not need the details to carry out their legitimate Trust duties.

Personal Responsibility & Accountability

Each member of staff has a personal responsibility to ensure that information is kept safe and secure at all times.

Whilst working at home, all staff must still comply with any Trust policies or procedures and any breach of these procedures will result in the same action as if it had occurred within Trust.

It is essential that any member of staff working from home is aware of the relevant Trust policies e.g. Data Protection Policy, Information Security Policy and Home Working Policy and completed the online Information Governance training.

Home Working Arrangements

When working from home consideration needs to be given to the following:

- **What information is required?** - Do not remove any hard copy information from the Trust premises. Consider what you need and check that you can access it through the secure Google Drive.
- **Recording** - If any paper records are required to be removed, ensure a record is kept of any information taken out of and returned to the Trust. This way it will be clear who has what information and for what purpose. In the event of a breach, this can help in identifying exactly what information has been compromised and how the impact can be managed.
- **Format** - If the information is in hard copy, would it be possible to take an electronic copy? This way the information will be stored on an encrypted device and if lost or stolen, will cause no impact on any named individual.
- **Transit** - When on route to or from home, you must ensure information is secure. Do not leave paper records, laptops etc on the seats of vehicles. Always store them in a secure place e.g. the boot of your car and keep it locked. Consider the use of secure and lockable cases for the transportation of documentation. Go straight home and remove the information from the car, before going on to the shops etc.
- **Location** – When working at home, ensure the location is suitable and away from other members of the household. This will help prevent any unauthorised access to paper or electronic records. Viewing information on a screen is "processing" and unauthorised people reading a screen containing personal information would be classed as unlawful obtaining or disclosure.
- **Paper documents/files** – Should not be removed from Trust premises and if they are, should be locked away in brief cases or secure filing cabinets when not in use. Prints should be collected from printers as soon as they are produced and not left where they can be casually read.
Never leave papers, files or any device in the car overnight. Always keep the information or device secure in your house. It is also advisable not to keep the paper records with the electronic device. In the event of a burglary, a thief will target electronic devices and therefore by keeping paper records separate this will reduce the impact of any theft.
- **Computers and mobile devices** – Should be password protected. When not in use they should be switched off. If only leaving the computer for a short period, ensure the screen lock is activated. Sometimes short interruptions turn into long ones and the personal information should be protected during the absence of the authorised user. Close up your device when you leave it for any period of time.
- **Equipment** – Should not be left where it would attract the interests of the opportunist thief. In the home, it should also be located out of sight of the casual visitor e.g. not left in the hallway.

It is appreciated there will be times when there will be a need to work from home especially when social distancing/shielding or in the event of an outbreak. You should use your chromebook/laptop provided by the Trust in preference to your own home device.

Any member of staff who works from home and uses their own ICT equipment must not hold any database, or carry out any processing of personal information relating to the Trust.

This would include emailing personal information to a private email address to be accessed later through non-Trust equipment. If a shared home computer is going to be used to e.g. access the Trust MIS etc consideration needs to be given to the digital footprint that is going to be left e.g. cached files etc on the shared computer and any trace of these must be removed.

Never disclose information about an individual to other members of the family, friends or any other individual who does not have a need to know it.

Video Conferencing Checklist

When it comes to remote homeworking and video conferencing the ICO have issued the following guidance:

(1) *Has the Trust checked the privacy and security settings?*

Video conferencing technology must be transparent. Users need to know how their data will be processed, as well as having choice and control over it. So the Trust should make use of privacy and security features. These can include restricting access to meetings using passwords, controlling when people can join the meeting or controlling who is allowed to share their screens. Think about who and how you share the meeting ID or password.

Google Meet is used in preference for teaching and additional security has been purchased. All staff have been trained in its use, it has been thoroughly risk assessed and there are always 2 members of staff present.

Is the Trust aware of phishing risks in training?

Many of us are aware of the signs of phishing emails or texts, but would the Trust know what to look out for in a video chat? The 'live chat feature' can be used by malicious people to spread phishing messages. Be vigilant. Don't click on links or attachments you were not expecting or from meeting attendees you do not recognise.

Note there will not be any uninvited attendees in any meetings arranged by the trust.

(2) *Have you checked your organisation's policy?*

The Trust selected Google for Education, a video conferencing platform that matches its policies.

(3) *Have you ensured all software is up to date?*

One of the most effective security measures a Trust can take is to keep all its software up-to-date, and video conferencing software is no exception. All of the software will be kept up to date by the IT department.

(5) Is this still the right tool for the job?

The Trust had already been using Google for Education before Covid hit and it had been tried and tested. We have no reason to doubt that it is still the right tool for the job.

In Summary

The Trust has considered balancing these considerations with what personal information is transmitted over video. No data will be recorded over the video stream.

Additionally, wherever possible, the amount of personal data shared across the video conferencing platform will be kept to a minimum, especially where safeguarding and special category (e.g. medical) data is concerned.

Linkages with other Trust policies

Remote home working will link with a number of other Trust policies including the following:

- Acceptable Use Policy
- Data Protection Policy
- Information Security Policy
- Safeguarding and Child Protection Policy

Disposal of Paper, Media and Equipment

Equipment that is no longer in use must be disposed of via the process that the Trust has in place.

Any paper documents containing personal information, which are no longer required, should be disposed of under secure conditions. Paper items containing personal or sensitive data must not be placed in household rubbish unless they have first been shredded via a cross cut shredder.