Data Protection Guidance for Home-Working during the COVID-19 response

THE MID AND WEST WALES SAFEGUARDING BOARD

2nd April 2020

Purpose of this Document

This document has been created to remind staff of best practice when working from home, in light of the measures being taken to contain COVID-19 through more flexible working arrangements.

This guidance is for advisory purposes only, and the responsibility for information governance and compliance with GDPR requirements and legislation remains with each agency in the partnership. Staff should read this document alongside their own agency's guidance and Data Protection Procedures.

Work Area

Be mindful of where you are working and discussions being undertaken. Consider anyone else in your household in terms of where you set up your workspace. No-one else should be able to see your screen or paperwork, or overhear confidential discussions. It may not be possible to prevent this completely; but every effort should be taken to minimise risk of others in your household hearing/seeing confidential information.

You should also bear in mind windows and whether anyone outside can hear phonecalls/see your screen. Lock your computer screens when away from the desk/location, however briefly you are leaving the workspace.

Be mindful of paper records and keep them secure at all times. Avoid leaving them out and visible to others in the household; if you can, lock or store them away in a drawer.

Methods of Communication

Communication with colleagues which involve personal data should be through usual work channels only, e.g. phones/Skype/work email etc. Avoid use of other channels such as Facebook messenger as these rarely use encryption services to protect data in transmit, unless agreed by your organisation. **NB: it is the responsibility of organisations to ensure any approved communication platforms are secure and encrypted.**

Skype / Microsoft Teams Meetings

Consider who is invited to calls discussing confidential information and keep this to a minimum; avoid bolting-on confidential discussions to team/group meetings unless everyone on the call is a necessary recipient of that information. Check at the start of the call who is taking part and take care when setting up calls to ensure the correct individuals are invited.

Recordings should only be made when necessary to do so and all parties are in agreement.

Email

As we rely more heavily on email, keep practice as robust as possible in terms of checking that the email addresses of recipients is correct. One of the most common data breaches occur as a result of selecting the wrong name in a contact list, or self-populated suggestions e.g. clicking David John instead of David Jones. Auto-Populate of recipients can be turned off and should be considered as a means of reducing the risk of this.

If you need to send any confidential information via email, keep the body of the email free of anything which identifies a customer, and instead contain all of the personal information in an attachment which you then password protect. If the information you are sending is sensitive, best practice would be to password protect this data to reduce the risk of someone else accessing it.

If you are sending anything with a password, do not include the password in the email. Ideally, give the recipient the password via other means, e.g. asking them to call you for it wherever practicable.

If you are sure of and have checked the recipient, then organisational email encryption can be employed, such as Microsoft Encrypt or TLS

NB: encryption systems on email servers protect against external interception of messages, but do not protect against unintended recipients within agencies from accessing the data.

Auto forwarding organisational emails to personal email accounts is not acceptable, and avoid using personal email accounts wherever possible; these do not have the same encryption or protection as work accounts. If this is not possible in the current COVID-19 context, use the most secure method of protection available.

Personal Devices

If you have no option but to use a personal laptop, ensure you have anti-virus software. If this device is shared with others in your household/family, keep all confidential information password-protected under your own user account or area. Do not select “remember me” options for work-related login details on a shared computer or account, and make sure that you log off after each session in any work-related programmes or sites so that they cannot be accessed by any other users of the computer.

Where in place, the organisation’s Bring Your Own Device policy must be followed.

School staff can and should make use of the storage area available on Hwb which enables secure and password-protected storage of data.

Save all documents to servers instead of desktops, to ensure the data is backed-up and secure.

Other Considerations

- Keep your passwords secure and confidential and change them frequently.
- Avoid use of memory sticks to save files, but where these are employed ensure they are encrypted.
- If visiting customers, be mindful about what paperwork you take and restrict this to the paperwork required for the visit(s) being undertaken only.
- When in transit equipment or paperwork should not be left in sight in unattended vehicles.
- If you think that there has been a breach of personal data, you should report this following your agency's Data Breach Procedure.