Working at home, a guide to GDPR

John Taylor MAT

Many staff across our trust work from home or at a location which it not their home school, whether that be marking students' work, planning, financial planning/reporting or for general administrative activities. When working from home you and the trust are still required to ensure personal data is safe and secure under the Data Protection Act (DPA) and the General Data Protection Regulations (GDPR). This guidance is document aims to offer some practical advice on how to achieve that.

What is personal data?

'Personal data' means any information relating to an identified or identifiable living person (often referred to as the 'data subject'); an identifiable living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, UPN or admissions 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 person.

Find out more: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

How do I comply with the DPA and GDPR at home?

Complying with the DPA and GDPR at home can feel daunting, by following these simple steps below you be confident with your use of data:

- Apply the common sense test and ask yourself the question: If this way my personal data would I be happy for it to be stored, left out or used in a particular way? If the answer is 'no' modify the way you are working.
- Do not leave personal data in your car or on public transport.
- Ensure data is stored in a safe and secure location when not in use, not left out on the table.
- Do not save any information onto a personal computer or mobile device.
- Do not share you password or if provided staff device with anyone.
- Ensure your screen cannot be read by others, this applies to mobile devices where you might read email as well as laptops.
- Avoid printing documents. If you are required to print a document ensure it is stored securely.
- Do not save any passwords or tick "stay signed in" when accessing websites or other resources.
- Exit all applications when you have finished working.

What should I do if I think a data breach has occurred?

If you think a data breach has occurred for example someone else at home has read documents containing personal information this must be reported to the Data Protection Officer (DPO) via email dpo@jtmat.co.uk. You should include the following information in your email:

- Your name
- A contact number should the DPO need to speak to you
- A description of the records that have been breached e.g. IEP, attendance certificate or payroll document
- A description, in your own words of the breach, how it occurred and how you came to be aware.

Please do not attach any documents to your email. These will be requested if required.

What should I do if I'm unsure of my responsibilities or have any questions?

If you are not sure about anything please contact the trust's Data Protection Officer via email dpo@jtmat.co.uk.