

Colleagues,

We all expect our data to remain private and only be used for necessary purposes. We must treat our service user and staff data as we would expect our own to be treated. New legislation came into effect in May 2018, (the GDPR and Data Protection Act 2018), which enhanced the rights and expectations of individuals in terms of how their data is processed. This list of Do's and Don'ts can help staff understand how to process personal data correctly.

Do:

- Know who your Information Asset Owner (IAO) is (Commonly a Head of Service)
- Know how to contact the Trust's Data Protection Officer
- Know why you are processing personal data
- Know how to recognise and report a personal [Data Breach](#)
- Use encrypted laptops and secure them when taken outside the office
- Know how to recognise a [Right of Access](#) request and what to do.
- Treat someone's personal data how you would want yours to be treated; carefully, legally.
- **THINK AND CHECK BEFORE YOU SHARE**

[Department of Health Short Video Data Protection Do's and Don'ts](#)

Don't:

- Share personal data without a valid, legal reason
- Give out personal data over the phone if you are not sure who you are speaking with
- Post data on colleagues or customers on Facebook or other social media sites
- Send e-mails to large groups of people without considering using bcc (blind carbon copy) facility
- If in doubt – don't share personal data – check with your IAO/DPO
- Don't access records unless you have a legitimate business reason to do so.

Not following data protection rules, guidance and policies exposes the Trust to the risk of a data breach.

Examples of a Data Breach:

- Sending a service users' letter to the wrong address (if they have given us the right address).

- Sending Service User A details of Service User B (accidentally including their papers in the envelope / grabbing wrong papers from the printer without checking etc).
- Giving personal details of a Service User over the phone to someone who cannot prove that they are the Service User or that they are acting on their behalf and with their consent.
- Discussing a Service User's personal details with someone not entitled to know those details – a friend, colleague, family member etc.
- Leaving personal information unsecured within your office.

Should you experience a breach, or suspect one may have occurred you should follow the Trust's guidance, '[Action to be taken in the case of a security breach](#)'.

Further Information

Further data protection guidance and information is available on [SharePoint](#), or contact the [Information Governance Department](#)