Staff Guidance on Data Breaches

1. What is a data breach?

A data breach is when the information we hold, create, or share (e.g. care records) is compromised. This might be in one of 3 ways:

1.1 **Confidentiality** – When a person gains access to information they shouldn't have. This might be malicious i.e. a hacker, or it might be a simple mistake i.e. sending an email to the wrong person.

1.2 **Integrity** – we need to know that information is accurate and that it was created by the right person. For example, a MAR sheet needs to have been filled out correctly. If there is an error on the sheet – whether on purpose or not – this is a data breach; or

1.3 **Availability** – for data to be useful we need to be able to access it. If it isn't available this is also a breach, e.g. there is a care record which is needed to provide care for someone, this is kept locked in an office, if the keys go missing and no one can access that record then this is a data breach.

2. What should I do if there is a data breach or I think there is a data breach?

It is better to report a breach even if you are not sure that it is one. As with incident reporting, near misses are as important to report as actual incidents. This is how we learn and can hopefully prevent these things happening in the future.

What to do:

2.1 If you believe a crime has been committed, someone has been injured, or an intruder is on site contact the emergency services via 999.

2.2 Fill out a Data Security Incident Report Form immediately. This can be found here. This form will be sent to the Data Security and Protection Lead **or equivalent job role.**

2.3 If you have identified a potential security breach, inform your line manager or Data Security and Protection Lead **or equivalent job role** at the earliest opportunity.