

Training needs analysis

Template v1

**For staff**

| Area of training | Types of staff | Staff member name | Staff member name | Staff member name | Etc |
| --- | --- | --- | --- | --- | --- |
| Data and cyber security awareness and good practice, including: * Data protection
* Data quality
* Record keeping
* Data security
* Confidentiality
* Rights of individuals under GDPR including subject access requests
 | AllFrontline Care StaffOffice StaffManagersBoard members |  |  |  |  |
| Physical security including paper records and files | All |  |  |  |  |
| Preventing data and cyber security threats including awareness of potential threats, and reporting incidents (data breaches) including near misses | All |  |  |  |  |
| Email good practice | Staff who use email |  |  |  |  |
| Password good practice | Staff using passwords to access company systems |  |  |  |  |
| Safe use of removable media (memory sticks) with company computers | Staff using computers to do their work |  |  |  |  |
| Safe use of company laptops, tablets and phones | Staff provided with company devices |  |  |  |  |
| Safe use of personal mobile phones to carry out company business | Those who use generic systems such as WhatsApp for work or who use an App to view care records using their own phones. Those who access company email and/or documents or systems from their own devices. |  |  |  |  |

## For staff with responsibility for data security and protection

| Area of training | Types of staff | Staff member name | Staff member name | Staff member name | Etc |
| --- | --- | --- | --- | --- | --- |
| DSPT | Data Security and Protection Lead, managers |  |  |  |  |
| Business continuity planning and data protection impact assessments (DPIA) | Data Security and Protection Lead, managers |  |  |  |  |
| Software updates  | Data Security and Protection Lead, managers |  |  |  |  |
| IT infrastructure, including: * Operating system updates
* Backups
* Firewalls
* Anti-virus software installation/updates
* Network management (if a network of computers is in place)
 | Internal or external IT support. If there is no IT support then the Data Security and Protection Lead or manager may require training |  |  |  |  |
| Secure use of company hardware:Encryption PINs and two factor authentication Remote tracking/wiping of mobile devicesLimiting downloads to verified software | As above |  |  |  |  |
| Setting up user accounts and control of access to which parts of systems | As above |  |  |  |  |