

Data Security Audit Checklist

Template v1

This checklist is a guide which you might chose to use – you can add or remove these checks from your audits as applicable for your organisation.

|  |  |
| --- | --- |
| Staff  | Date audited |
| Spot check that staff understand their responsibility towards data security  |  |
| Spot check that staff are aware of our data protection policies  |  |
| Have staff received training on data protection?  |  |
| Have any staff undergone disciplinary action in relation to data protection and security?  |  |
| Spot check that staff understand how to report security breaches and near misses.  |  |
| Physical Access to hardcopy records  |  |
| Check the record of which staff have access to confidential areas is up to date.  |  |
| All offices, files, or cabinets which contain confidential information are kept locked when not in use.  |  |
| Has all confidential waste been disposed of securely and are there destruction certificates? (If applicable)  |  |
| Has anyone inappropriately accessed, or attempted to access, confidential records?  |  |
| Digital Access to records  |  |
| Is the allocation of administrator rights restricted?  |  |
| Have staff access rights been reviewed?  |  |
| Check if there is any evidence of staff sharing access rights.  |  |
| Screens are locked when not in use.  |  |
| Check that our password policy is being followed  |  |
| Has anyone inappropriately accessed, or attempted to access, confidential records?  |  |
| Have appropriate security measures been applied to all computers, laptops and mobile devices?  |  |
| Staff are using computers appropriately e.g. no personal use, no downloading unapproved software, no social media use etc.  |  |
| Sharing data  |  |
| Our procedures for safely sharing personal information via post are being followed.  |  |
| Our procedures for safely sharing personal information via fax are being followed.  |  |
| Our procedures for safely sharing personal information via secure email are being followed.  |  |
| Legal Checks  |  |
| The Information Asset Register has been reviewed and signed off.  |  |
| The Record of Processing Activities has been reviewed and signed off.  |  |
| Records of consent are up to date and still applicable.   |  |