

SECURITY CHECKLIST FOR PERSONAL DATA

This checklist is only a guide to assist the school in identifying its security measures and requirements in respect of personal data. There will be a need to raise awareness of security for both data and computer equipment, which may hold/access personal data.

Physical Security

	Yes	No
Do you have access controls to the school? (What are they? - access controls should be documented/recorded)		
Do you have access controls to the office/rooms? (What are they? - access controls should be documented/recorded)		
Do you lock filing cabinets which store manual files? (Who have access to these cabinets/storage areas? - document)		
Does anyone, outside your school, have access to these cabinets or files? (Who are they?)		
Is there a security alarm system for the building?		
Do you have a list of keyholders? (Record list of authorised holders)		

Computer Systems

	Yes	No
Is personal data stored on computer systems?		
Are computers/terminals sited in lockable rooms when unattended?		
Are the computers/terminals switched off or logged off when not in use or when left unattended?		
Is access to computer equipment limited to authorised personnel? (who are they?)		
Is there password protection to the equipment and applications?		
Is there password protection to data?		
Do all authorised users have separate LOGONS?		
Are Logons disabled when people leave or when a breach is suspected?		
Are the passwords kept confidential?		
Are there adequate software controls to the personal data other than passwords; (i.e. restriction of access for input, amend, delete and enquiry)		
Are the access rights/user privileges to personal data, or equipment holding personal data, taken away after staff who have left the school's employment?		
Are backups of data carried out frequently?		
Are disks, magnetic tapes removed and locked away when not in use?		
Do you regularly review access levels?		
Is there a person responsible for data, software control and hardware security?		
Is the software held on the computer proper and legal and not a copy taken from another computer?		
Do you or your staff take the computers (which hold personal data) off-site?		

Operational Security

	Yes	No
Have you completed the Data Protection Notification Process for the school? (Ensure a record of the notification is maintained and annually renewed)		
Are staff aware of the Notification details? (what data is used for, disclosed to, etc)		
Have staff been informed of the obligations of the Data Protection Act?		
Are staff regularly reminded that they must not release personal data to anyone not covered by the Notification?		
Is personal data taken off-site by anyone in the school? Do you have a list of authorised personnel.		
Are there adequate security measures in place to protect personal data that is taken off-site?		

Operational Security (cont'd)

	Yes	No
Do you regularly train staff on security procedures?		
Are instruction booklets, papers, files or manuals describing or holding personal data locked away when not in use?		
Is the access to the instruction booklets, papers, files or manuals limited to authorised personnel only? (i.e. not borrowed or easily copied)		
Are old copies of instruction booklets, papers, files or manuals securely destroyed or shredded?		
Are computer printouts of personal data secured (i.e. not accessible to unauthorised personnel)?		
Are old printouts securely destroyed or shredded?		
Is there a list of authorised users for computers and data, and their access rights?		

Records Management

	Yes	No
Do you have a "Records Management Policy"?		
Do you know what records you have? If not, you should consider carrying out an "Information Audit" and compiling a "File Register"?		
Do you regularly review your records and arrange for "disposal" in line with the "Schools' Disposal of Records Schedule"?		

Action Required:

If a 'YES' answer is ticked, then documentary evidence should be maintained and regularly reviewed to show compliance.

If a 'NO' answer is ticked, then further action may be required.

Documentary evidence should be maintained by the school in relation to the above issues.

Guidance is available from www.seelb.org.uk