Whitgreave Primary School
Information Security Policy and Guidance Notes

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance of relevant Information Governance Legislation.

Taking measures to protect records can ensure that:
• Whitgreave Primary can demonstrate compliance with the law and avoid data loss incidents.
• In the event of a major incident, Whitgreave Primary should be able to stay open and will at least have access to its key administrative and teaching records.

This Information Security Policy should be read in conjunction with the Whitgreave Primary's Business Continuity Plan and should deal with records held in all media across all school systems:
• Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images).
• Hard copy (including but not limited to paper files, plans).

Digital Information
In order to mitigate against the loss of electronic information Whitgreave Primary School must:

a) Operate an effective back-up system
Regular backups of all information held electronically are undertaken to enable restoration of the data in the event of an environmental or data corruption incident. These backups are stored in a different location to the servers off the main school site. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible.

b) Control the way data is stored within the school
Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software.
Staff should be advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

c) Maintain strict control of passwords
Ensure that the data is subject to a robust password protection regime, ideally with users changing their passwords every 30 days. Discourage password sharing strongly and seek alternative ways for users to share data – like shared network drives or proxy access to email and calendars.
In addition, staff should always lock their PCs when they are away from the desk to prevent unauthorised use.

d) Manage the location of server equipment
Ensure that the server environment is managed to prevent access by unauthorised people.

e) Ensure that business continuity plans are tested
Test restore processes on a regular basis to ensure that the first time you identify a problem with the backup is not the first time you need to retrieve data from it.

Hard copy information and records
Records which are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.

a) Fire and flood
The cost of restoring records damaged by water can be high but a large percentage may be saved, fire is much more destructive of records.
In order to limit the amount of damage which a fire or flood can do to paper records, all vital information should be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water.
Where possible vital records should not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood.
The bottom shelves of a storage cupboard should be raised at least 2 inches from the ground.
Physical records should not be stored on the floor.

b) Unauthorised access, theft or loss
Staff should be encouraged not to take personal data on staff or students out of the school unless there is no other alternative.
Records held within the school should be in lockable cabinets.
There should be restricted access to offices in which personal information is being worked on or stored.
All archive or records storage areas should be lockable and have restricted access.
For the best ways of disposing of sensitive, personal information, see the guidance notes on Safe Disposal of Records

c) Clear desk policy
A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/or flood damage.
A clear desk policy involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

Disclosure
Staff should be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it. Ensure that where you intend to share personal information with a third party that you have considered the requirements of the General Data Protection Regulations. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address which can be verified.
Where appropriate you should develop a data sharing protocol with the third parties with whom you regularly share data.

Risk analysis
Whitgreave Primary School should undertake a business risk analysis to identify which records are vital to school management and these records should be stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks.
The development of an information asset/risk register can assist with this process.

Responding to incidents
In the event of an incident involving the loss of information or records, Whitgreave Primary School should be ready to pull together an incident response team to manage the situation.
Whitgreave Primary School should consider assigning a specific member of staff to deal with press/media enquiries.

a). Major data loss/information security breach
Whitgreave Primary School should have a process which must be used by all members of staff if there is a major data loss or information security breach. This will involve appointing a named member of staff to liaise with the Information Commissioner's Office if an information security breach needs to be reported.

The General Data Protection Regulations require organisations to inform the Information Commissioner's Office within 72 hours of being notified/being aware of a breach occurring. All potential instances are to be notified to the named contact within 48 hours so that an informed decision can be made relating to the incident.
Do not put off informing the Information Commissioner's Office if the incident is serious enough to justify notification. It is better to have notified the Information Commissioner before someone makes a complaint to him.

b). Fire/flood incident

You should create a team of people who are trained to deal with a fire/flood incident. This will include the provision of an equipment box and the appropriate protective clothing.

The team and equipment should be reviewed on a regular basis.