Barlborough Primary School

ICT DISASTER RECOVERY AND SECURITY PLAN
Updated October 2018

Authorised access to RM Integris:

Headteacher :- Mrs Kerry Towndrow-Birds
School Office :- Mrs M Riley
Network manager:- Mr. D Smith
All teachers (need access in order to complete registers)

Access to the administration system is limited to known individuals via passwords. Only the above authorised personnel have access to children's and parents' data apart from authorised personnel from Social Services and Education Social Welfare departments.

Please note the Data Protection Act allows disclosure of personal information to other bodies such as the Local Education Authority, Connexions etc. Care should be taken when disclosing personal information.

The school is registered under the current Data Protection Act.

All data for management purposes is backed up regularly by the ICT technician. Two current copies of all management data are kept in two separate secure locations. Backups are also encrypted using Veracrypt. School uses a web based management on-line system which does not need backing up by the school

Windows defender software is installed on all computers and is regularly updated from the internet.

Authorised access to SAP and OrderPoint

Headteacher :- Mrs Kerry Towndrow-Birds
School Office :- Mrs M Riley
Deputy Headteacher: - Miss Amanda Gee

Access to the finance system is limited to known individuals via passwords.

Authorised access to PerspectiveLite

Headteacher :- Mrs Kerry Towndrow-Birds
School Office :- Mrs M Riley

Access to PerspectiveLite is limited to known individuals via passwords.

Curriculum Network

The network manager, ICT technician and ICT Co-ordinator ensure that pupils save their work to the network and not to local drives or external drives. Staff are also encouraged to save to the network. Students work is backed up on a regular basis to enable recovery in the event of the loss of data files or system failure. Backups are on external hard drives; they are rotated on a weekly basis and stored either in a fire-proof safe or in a separate building to the Server. The back up log on the server is checked regularly by the ICT technician, to ensure that the back up has been carried out successfully.

*Management hardware and the Server system network are covered by a maintenance contract with our Primary Cluster ICT Technician. Therefore server operating systems and drivers will be reinstated by them and all software and hardware will be replaced and re-loaded in the event of failure, theft, etc. All Schools important data will be on the backups. Certain softwares e.g. Micorosoft Office are carried by the Network manager and the IT Technician through MS Volume Licensing agreement and will be re-installed after any disaster.

The school has Virus protection installed on all computers including the server. The virus protection is regularly updated from the Internet and all staff are aware of the importance of allowing the updates to proceed. If a virus is identified by a computer then this is reported immediately to the ICT Coordinator or ICT Technician who will take action to remove the virus. The infected computer should not be used until the virus has been removed (unless the Antivirus tells the user it has quarantined the Virus or Malware).

The school regularly downloads the Windows Update for the server and each computer on the network.

All staff are aware of the Internet Use and E-mail regulations and Acceptable Use Policy.

Storing Information

All staff are encouraged to save their work on the school network so that this is backed up regularly. Only encrypted memory sticks are to be used in school to support the transfer of information. Teaching staff are issued with encrypted laptops in order to meet GDPR and data protection regulations.

For Insurance Purposes

All computers, printers, equipment etc. are listed on the School Inventory, with serial numbers and other relevant information. These inventories are maintained regularly by the network manager, ICT technician and school office and checked annually by the Head. Software licences are listed and maintained by the network manager and ICT technician. The insurance company is kept informed of acquisitions of new equipment (as dictated by the policy covering the school).

The network manager/ICT technician together with the Head Teacher are responsible for carrying out the disaster recovery plan.

In the event of a disaster staff, pupils and support services are kept informed of the situation.

The disaster recovery plan is tested and updated regularly.

Staff are aware of the existence of the Disaster Recovery Plan.

In the Event of a major disaster:

According to the nature of the incident, an outline recovery plan will need to be prepared and actions prioritised by the network manager, ICT technician and / or Headteacher. An event log will be started and maintained and all key events will be recorded. Any follow up action will also be recorded. The disaster recovery plan should be reviewed as a result of this log.

Rating	**Business Impact**	**Recovery Time Objective**	**Recovery Point Objective**
Critical	Immediate	Within 4 hours	No data loss preferred. Minimal data loss might be acceptable.
High	Significant within 4 hours	Within 8 hours	Minimal data loss
Medium	Significant within 24 hours	Within 24 hours	Minimal data loss
Low	Business could survive for 24 hours, or even days.	Within 48 hours	Minimal data loss preferred. Upto last daily backup might be acceptable