Furness Vale Nursery & Primary School

Computer Disaster Recovery Plan

'This policy has been reviewed on 08/12/2021 and has been impact assessed in the light of all other school policies and the Equality Act 2010.'

DATE AGREED	REVIEWED ON	NEXT REVIEW	COMMITTEE	MINUTE NO	SIGNED
08/12/2021	**08/12/2021**	**08/12/2022**	**FGB**	**21/63**	**K.GILL** **H.PIKE** **C.WARD**

COMPUTER DISASTER RECOVERY AND SECURITY PLAN

Furness Vale Nursery & Primary School is committed to developing the use of ICT throughout the School organisation and to developing the skills and knowledge of both staff, students and the wider community. The School Staff Acceptable Use Policy gives further information and advice.

In the event of a major disaster resulting in the loss or unavailability of systems and/or data the IT Disaster Recovery and Security Plan will be implemented in conjunction with the Critical Incident Plan.

The school comply with the Data Protection Act.

Misuse of Computers

All staff and pupils are required to comply with the Computer Misuse Act 1990. A copy of this is available to download or view from www.legislation.gov.uk

Particular attention is drawn to Section 1 of the Act which states:

"A person is guilty of an offence if:

a) she/he causes a computer to perform any function with intent to secure access to any program or data held in a computer and
b) the access she/he intends to secure is unauthorised and
c) she/he knows at the time when she/he causes the computer to perform the function that this is the case".

(In other words knowing that they are not authorised to access certain programs or data, and they continue to do so).

All staff and pupils are informed to only use their own id and password at all times. Any requests for this information are to be refused.

Staff are advised that an offence under the Computer Misuse Act 1990 is a serious issue and anyone convicted of such could be liable to a fine, imprisonment or both.

Use of the Internet

- Internet access will be available to staff and students via laptops/pcs/iPad etc., connected to the School and administration network where considered appropriate.

- All members of the School community and visitors to the School are expected to use the Internet in an appropriate manner at all times.

- If students or staff discover unsuitable material, the URL and the nature of the content should be reported immediately to the ICT Technician, School Business Officer or the Headteacher.

- The School e-mail is checked on a daily basis by the School Business Officer who ensure the e-mails reach their required destination. This only applies where mail has come direct to

their own school email address for a member of staff or enquiries@furnessvale.derbyshire.sch.uk

- Any member of the School community or other School user who, in the opinion of the Headteacher, uses the Internet inappropriately will have their Internet access rights removed.

Computer Access - Passwords and Security

AUTHORISATION AND ACCESS

- Levels of access will be established for different users on the various networks and systems operating in School. **(Appendix 1)**

- Responsibility for maintaining and monitoring access and authorisation will be as follows:

School Network (Curriculum)	ICT Co-ordinator in consultation with the DCC ICT Technician
Broadband connections	School Business Officer in consultation with the Service Provider and ICT Technican
Administration Network	School Business Officer in consultation with the Headteacher
RMIntegris	School Business Officer in consultation with the Headteacher
SAP (Finance & Ordering)	School Business Officer in consultation with the Headteacher
School Website	Headteacher, School Business Officer and It Support

Access to systems and data on computers is restricted by the use of unique identifiers and passwords.

- All staff must follow a password protocol as follows:

  - Keep your password confidential.
  - Do not write down your password.
  - Do not let others use your ID or password.
  - Passwords should be at least 8 characters in length, contain a mixture of characters, changed upon first logon and periodically thereafter.
  - Do not leave the computer logged on when you leave it for any length of time.

- Access to the server is limited to nominated personnel, currently the ICT Technician, DCC IT and the School Business Officer. All data is encrypted and the service level agreement with DCC is updated annually.

- Users who no longer work at the school will have their access rights removed at the time of leaving.

Access to confidential data systems is limited to known individuals via an identity code and password (usually a DCC Payroll number) Staff are reminded to keep their password secure and not to use any other person's ID or to let them use yours. Only named authorised school personnel have access to children's and parents' data.

The Data Protection Act allows disclosure of personal information to other bodies such as the Local Education Authority, Social Services and Education Welfare department. Care should be taken when disclosing personal information. A copy of the Data Protection Policy is available from the School Office. The school is registered under the current Data Protection Act.

User accounts for **SAP** (Finance and Ordering System) are managed by the corporate applications team. The Headteacher will submit requests to the SAP in Schools Team using the appropriate forms available on the Learning in Derbyshire website to add/edit/delete users. Logon details will be provided to individual users and must not, under any circumstances be shared with anyone else.
Any former employees of the school and anyone who no longer needs access to systems are deleted as users at the time of leaving employment at the school.

User accounts for **RM INTEGRIS** (MIS) are managed by the School Business Officer Logon details are provided to individual users and must not under any circumstances be shared with anyone else. Any former employees of the school and anyone who no longer needs access to systems are deleted as users at the time of leaving employment at the school.

Access levels to SAP / RM Integris / LiD and the School Network are set as appropriate for each user by the Headteacher. Individuals do not have access to systems and data to which they are not authorised to view.

Access to the 'Alfresco' files/folders used for administration purposes is restricted and can only be accessed by authorised personnel. Access rights are set up by the IT Technician in consultation with the Headteacher and School Business Manager.

Computer Access information is attached. **(Appendix 1)**

Data Backups

SAP does not require the school to carry out any upgrades or backups as these are managed by the Corporate Team and Derbyshire County Council.

RM Integris is the online Management Information System (MIS) currently used by the school. As this is a web based system, upgrades and backups are managed directly by RM.

Admin, Staff and pupil documents are saved to Alfresco.

IT Just Done would be responsible for the recovery and re-installation of essential data in the event of loss of data files or system failure. The Schools IT Technician would assist with this process.

The Server together with all management hardware and software is covered by a contract with IT Just Done. Software including back-ups would be recovered and re-installed in the event of equipment/electrical failure, theft, etc from the I Cloud.

All computers, printers, equipment etc are listed on the School Inventory with serial numbers and other relevant information. The Inventory is maintained by the Headteacher with delegated responsibility. Periodic checks are made to ensure items on the Inventory are in school, all staff are asked to assist with this. When items are no longer in use they are written off the Inventory and Governor approval is required. Computer hardware is disposed of through an approved company. All data is removed by the IT Technician prior to this.

Antivirus software, is installed on the server as well as all school laptops and computers for both curriculum and admin. The computers are updated automatically. The teaching staff are responsible for ensuring that the antivirus software is maintained and updated on a regular basis on their school laptops. Any problems are to be reported to the ICT Technician or by informing the School Business Officer. Licences are updated as necessary.

Office, Teaching and Teaching Support Staff are all aware of the Acceptable Use Policy.

In order to maintain data protection and confidentiality, **all** Teaching Staff, Admin and Teaching Support Staff (where necessary) are supplied with encrypted memory sticks for all school related use. Staff are advised that no confidential data is to be stored on their laptop and that all documents should be saved on 'Alfresco'

Telephone numbers in the event of failure, theft or other emergency attached. **(Appendix 2)**

APPENDIX 1

IT DISASTER RECOVERY ACTION PLAN - COMPUTER ACCESS

SAP - Finance and Ordering System

SAP is a password protected programme and is accessed by the following members of staff via their payroll number and password. The programme automatically requests passwords are changed on a regular basis.

Name	Post	Level of Access
Ruth Parry	Headteacher	Approver
Tina Daniels	School Business Officer	Shopper/Payroll Inputter/Finance Monitoring & Reporting/All Entries for inventory/Invoices

RM Integris - Management Information System

RM Integris is a password protected programme and is accessed by the following members of staff via their payroll number and personal password. The programme automatically requests passwords are changed on a regular basis.

Name	Post	Level of Access

Ruth Parry	Headteacher	Admin Role
Tina Daniels	School Business Officer	Admin Role with full access
	All Teaching Staff	Teacher Role

SCHOOL EMAIL

Email addresses have been allocated to all staff. Staff are allocated a user name and password by our ICT support.

Email addresses can be allocated to children in school as required for curriculum purposes.

SERVER

Access to the Server is password protected. ICT support have access to the Server.

IT support have full access to the Server in order to carry out software installations and upgrades/maintenance/backups etc. An annual Service Level Agreement is in place for this.

APPENDIX 2

IT DISASTER RECOVERY ACTION PLAN - CONTACT AND OTHER RELEVANT NFORMATION

In the event of an incident which results in the loss of access to computerised systems, the IT Disaster Recovery Action Plan will come into operation. Depending upon the situation the following procedures will be followed, in conjunction with the Critical Incident Plan:

1. Contact **DCC IT** to install backups of server, reinstate broadband connection/email accounts and as necessary to PC's and Laptops and for reinstallation of DCC supplied software

2. Contact IT suppliers if replacement hardware required

ICT Software Audit - Admin		
Software Name	**Subject**	**Licencing Information**
RM INTEGRIS	MIS	Provided by RM
SAP	Finance & Ordering System	Provided by DCC
Microsoft Office Pro Plus	Admin/Curriculum	Covered by EES Licensing
Windows 10 (or current)		
Microsoft Endpoint Protection (Anti-Virus)		
Adobe	Admin/Curriculum	Free Software
Java		

KEYHOLDERS – Telephone Nos		
Name	**Post**	**Contact No**
Ruth Parry	Headteacher	
Chris Ford	Caretaker	
Toni Kania	ASC Co-Ordinator	07977156957
Kayleigh Gill	HLTA	

DCC - Telephone numbers in the event of failure, theft or other emergency	
Name	**Contact No**
DCC IT Helpline	01629 537777
CAYA School Support & Training	01629 536789
School SAP Helpline	01629 538088
DCC Property Services	01629 539929

IT Providers in the event of failure, theft or other emergency	
Name	**Contact No**
Joe McNulty	