Department for Education

Fioretti Trust

IT Backup Policy & Disaster Recovery Plan

Cyber Response Plan

Fioretti Trust

Last Reviewed	Jan-2026
Reviewed By	Jade Hunt – Savvy IT
Next Review Date	Jan-2027

Contents

1. Introduction

A Disaster Recovery Plan **(DRP)** for ICT Services is a requirement of the Academy Trust Handbook. It is reviewed annually or following any major changes to equipment or systems covered by the plan, to ensure it is always relevant and up to date.

Commented [HC1]: I think this should read 'Academy Trust Handbook'

Disasters are rare but when they do occur, they can have devastating consequences. This document looks at Disaster Recovery Plan for the Fioretti IT Team, and their ability to provide the contracted services provided in the event of a disaster or disruption to business. For the purposes of this plan a Disaster is defined as "loss or damage of part or all of Fioretti IT ICT infrastructure, which would have a high, or very high, business impact."

This document also includes the IT backup policy **(BP)** which compliments this disaster recovery plan.

Document Revisions and updates

Management of the document and plan

This document will be updated as required and reviewed after or yearly by the ISLT and Exec Team.

User	Date	Version
C Homer	04/02/2025	1.0

2. DRP - Activation of the Plan & Key Contacts

The plan is activated by one of the following:

- A member of the MAT Exec Team
- IT Services Lead Team (ISLT)

The IT Services Lead Team is responsible for the implementation of this plan. Progress and updates are reported to the Exec Team of the Trust and the Senior Team within Fioretti IT. In the absence of the IT Services Lead, the Exec Team will delegate the IT Services Lead role to the IT Hub lead or an alternative individual.

Commented [HC2]: Who is this?

Key Contacts when this plan is activated:

Name	Organisation	Role
	Fioretti Trust	Exec Team
Chris Homer	Savvy IT	IT Services Lead Team
	Fioretti Trust	IT Hub Lead
	Internet Company	
	Internet Company	

3. Key Services, Infrastructure & Passwords

Commented [HC3]: Should we have safeguarding software and MIS included on here?

Fioretti IT is designed to be flexible around its deployment – and as such our systems are designed to work anywhere.

System	Potential Risks	Mitigation	Inform
Access to IT Equipment or building	No access to Fioretti IT Equipment or offices	Any IT equipment can be used, and no access to Office is required	ISLT
Internet Access	No IT connectivity or MPLS Failure	Any internet connectivity, including home, another school, or 4G can be used	Savvy IT
Support Phone System	No access to helpdesk line	Direct line to Savvy IT Support	ISLT

Office365 Access (inc. SP/Teams)	Access to Office365 unavailable	No immediate risk, automated tasks completed manually or held.	ISLT
Website Hosting	Hosting failure. Site hacked.	Secure Logins and enhanced host security	ISLT
Arbor	Site offline. Site hacked. Users given incorrect access rights.	Essential contacts printed list. 2FA access to site. Data Backed up. Secure Logins. Access rights strictly controlled; admins can deny login.	ISLT
Access Finance	Site offline. Site hacked. Users given incorrect access rights.	Paper records for essential. 2FA for security access. Access rights strictly controlled.	ISLT
MyConcern / CPOMS	Site offline. Site hacked. Unable to login.	Paper records/secured printouts. 2FA for security access. Access via other admins or direct support.	ISLT

Passwords & Documentation

Passwords are stored within the IT support companies password management system. Multiple individuals have delegated access, with the senior team having overall access. Help Desk Team and Project Team have access to all sites at administrative level. All access is strictly 2FA.

Site Documentation is stored within the Help Desk Solutions, and available to logged in team members. Additional documentation can be found within the team SharePoint.

4. DRP - System Access & Risks

System & Access Risks

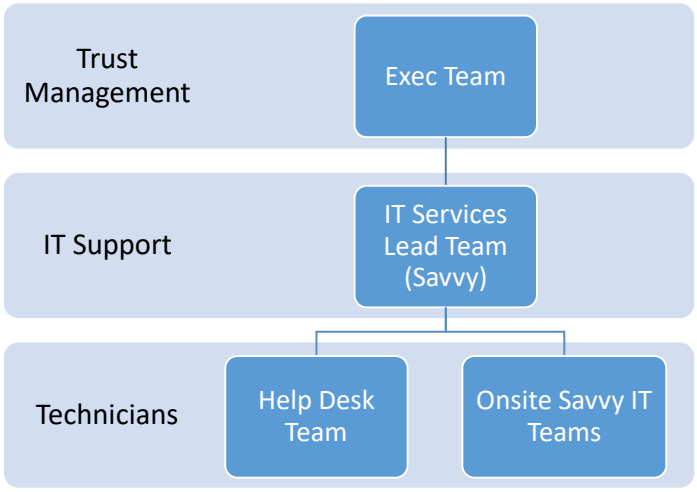
Legend

Likelihood	Severity	Negligible (1)	Minor(2)	Moderate(3)	Major(4)	Extreme (5)

Rare (1)		Low	Low	Low	Low	Medium
Unlikely (2)		Low	Low	Medium	Medium	High
Possible (3)		Low	Medium	Medium	High	High
Likely (4)		Low	Medium	High	High	Very high
Almost certain (5)		Medium	High	High	Very high	Very high

System	Event	Impact	Mitigation	Likelihood	Impact	Risk
VOIP System	Loss of access	Cannot answer calls	Split across 2 systems for redundancy. Other comms channels available.	3	3	9
Internet Service Provision	Loss of connectivity	Cannot access systems	4G availability or work offsite with laptop provision	2	2	4
Power/Network failure or loss of access to site.	Loss of connectivity	Cannot access systems	Laptops and 4G availability or work offsite with laptop provision, or work from a supported school.	1	3	3
Any used. (O365/ Internal)	Cyber Attack	Loss of access. Reputational Damage, inability to support. Data compromised	MFA implemented. Training provided to staff. Tough passwords monitored by 1Password for breaches. Multiple separations of escalation accounts to standard accounts.	4	5	20
1Password	Loss of Data	Loss of access to sites. Potential Security breach	Highly secure professional system with multiple steps in place to reduce risk.	1	4	4

Staffing



Staff Service Risk

Event	Impact	Mitigation	Likelihood	Impact	Risk
Key Staff unavailable	Loss of expertise	Clear Leadership structure to ensure continuity, documentation and shared access to resources	4	3	12
Rogue Staff	Vandalism of systems, or inappropriate access to data	Controlled access to mitigate risk to minimal systems.	1	4	4
Safeguarding Incident	Safety, reputation	Training and monitoring in place.	1	4	4

Contact Details

Contact details of key Trust personnel (as detailed in section 3) will be documented for easy access should the DRP be implemented for any reason. Fioretti IT Senior Team members or the Executive team, can access this information within Arbor.

Out of hours escalation procedure

On being informed of a major issue which is defined as an “Emergency”, members of the Exec Team or Hub Lead can contact Savvy IT to address the issue.

Less Urgent issues should be escalated via the school Headteacher, relevant Central Team Line Manager, who will escalate the issue to the correct staff or service providers.

5. DRP - Customer Liaison in the Event of Critical Issues & Key Communication Channels

Contact details of key Trust personnel and IT service providers (as detailed in section 3) will be documented for easy access should the DRP be implemented for any reason.

This documented information is stored in the Fioretti IT SharePoint and within the Fioretti HR Systems. Fioretti IT Senior Team members or the Executive team, can access this information within SharePoint.

In the event that SharePoint is unavailable, hard copies of these contacts details are stored at each Trust Central Hub and with the IT Services Lead Team, along with a hard copy of this DRP.

The ISLT team, alongside the Trust Head of Operations, will be able to quickly access these and contact the schools, or an alternative staff member in their absence.

Key Communication Channels

Email	Contained within Fioretti IT Website and mailing lists
Savvy IT Phone System	Pre-recorded messages
Website	Fioretti.co.uk
Onsite Staff	Communicate directly to schools
Teams	Communicate directly to Fioretti IT Team

6. BP - Definitions

Hot Copies – where backups are connected to the systems
Cold Copies – where backups are disconnected to the systems
Offsite backups – these can be a combination of hot and cold backups
Offsite definition – Offsite must be a separate site, and not include data on the same site.
Onsite definition – Backups connected to the production infrastructure.

7. BP – Specifications & Requirements

- User data:
  - **In Cloud –** a cold cloud backup to separate service.
  - **Local –** a local hot backup and a cold offsite backup.

- Servers:
  - **Configuration backups** – regular hot backups to be made.
  - **Servers Data** – hot and offsite cold.

Notes:

- It may be quicker to restore service by rebuilding servers rather than restoring backups, depending on the type of server.
- Cloud and some local Servers use versioning – this is not classed as a backup but can be used to restore files and folders from user error. It should be turned on for all shares (user and shared drives)
- Cloud Services will also be backed up periodically to comply with the requirements of the RPA.
- Software held on third party platforms, (EG Arbor, Access, My Concern/CPOMS and other cloud platforms) backup will be specific to the services provision, and this is why all software purchases or subscriptions should be signed with support from the IT department.

8. BP – Monitoring, Testing & External Support

Backup alerts are configured to email the helpdesk on failure. External providers will email reports which detail failures of backups to ISLT teams or relevant parties.

Backup and/or integrity testing occurs at the periods defined in the Backup Schedule.

8. BP – Backup Schedule & Data Security

Backup Schedule

School	Backup type 1 (hot and internal)	Backup type 2	Backup type 3	Testing

Primary Schools Servers	Backed up to NAS	Backed up to external HDD	Backed up to C2	Daily
Primary Schools Cloud	O365 Versioning. Constant.	Backed up to NAS. Daily.	Backed up to C2	Daily

Data Security

Backup type	Security measures in place
Cloud	Encrypted and stored in separate geographic locations or C2 Synology Cloud/Other Cloud providers.
Local	Local NAS boxes, secured and where applicable backups encrypted
Offsite	Encrypted to external USB. Password restricted and not shared with those carrying external backups. Stored centrally in fireproof safe,