Backup Checklist for Small Offices (UK)

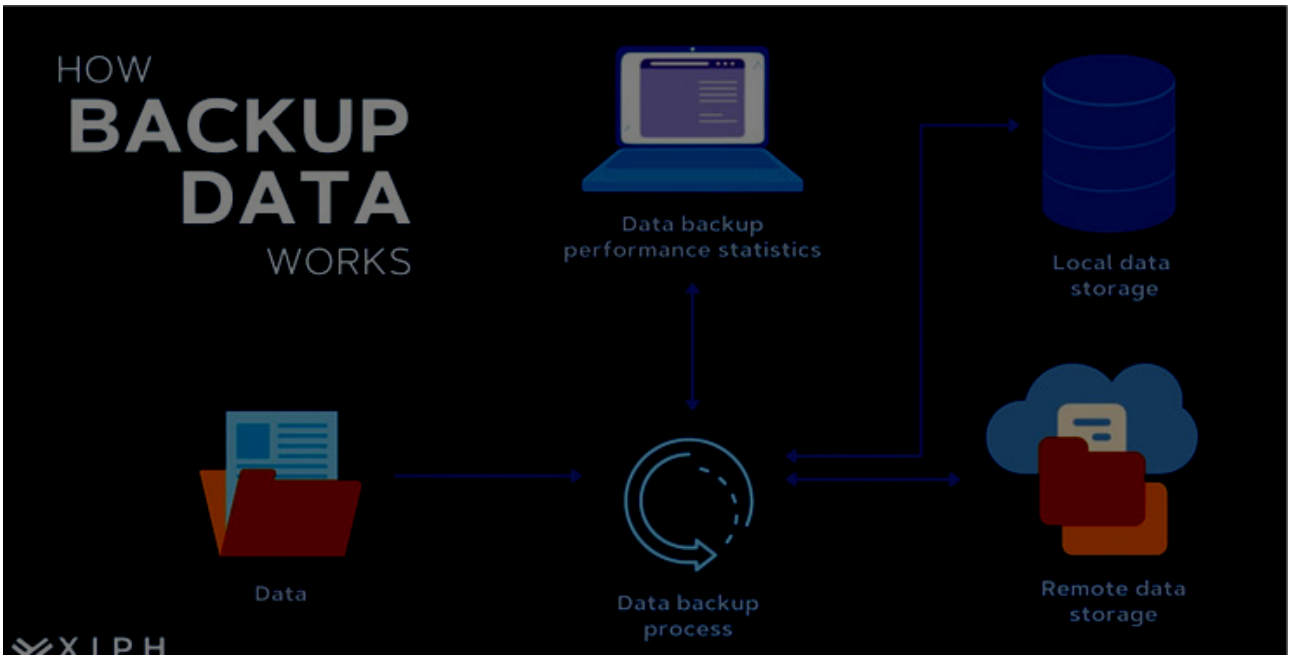
Simple, practical backup guidance for UK small offices

Prepared by
Computer Support Centre
https://computersupportcentre.com

Backup Checklist for Small Offices (UK)

Executive Summary

- What small offices should consider for backup solutions
- Not relying solely on life depending on the cloud services as means of backup is insufficient.
- It's imperative for small offices to create minimum quality standard for backup solutions.
- Backup solutions should help prevent lost productivity and the loss of data also.
- Essential, better and best practice for backup solutions.
- Five common failure points of backup systems in small businesses.
- Backup frequency recommendations and how to test backup systems.
- Who should be responsible for backup solutions in a small office.
- This checklist can be referenced as part of support for Cyber Essentials and GDPR compliance accountability.



Who this guide is for

This guide is for:

- Small businesses with locations in the UK and smaller size businesses that employ less than 50 employees.
- Office Managers, Office Directors, Team Leaders.
- Companies that do not have a dedicated IT expert.
- Companies that use PC's, laptops and Cloud Services to do business.
- Non-technical people that are looking for an easy-to-follow guide.

One-page: Minimum Backup Baseline for Small Offices

If your organisation does not do anything else regarding backups, the following items are the absolute minimum you must do to support your organisation's critical data:

- Identify all "Critical Data": Emails, Cloud Storage, Office Files, etc.
- Keep 3 copies of all Important Data.
- Store your backup data in at least 2 different locations.
- Maintain one copy of your backup offsite.
- Back Up Daily (Minimum).
- Maintain at least 30 days of Backups.
- Encrypt Backups and Limit Access to Backups.
- Test Data Restoration at Least Quarterly.
- A person should be responsible for backups.
- Document your backup storage and how to restore backup data.

The above items for Minimum Backup Baseline are in alignment with Cyber Essentials Best Practices and comply with the European Union's General Data Protection Regulation requirements for Data Availability.

Full Backup Checklist

1) What data needs backing up

Why it matters

You can only protect that which you understand and are aware of. Many small businesses back up their computers, but make the mistake of not backing up emails, data stored in the cloud or other applications that are critical to their daily operations,even when they do not understand the significance of these types of data.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
User files	Desktop & Documents	All work folders	Centralised storage	Office mgr	Daily	Avoid local-only data
Shared data	Manual copy	Automated backup	Versioned backups	IT/ops	Daily	Include permissions
Email	Provider retention	Dedicated backup	Third-party backup	IT/ops	Daily	Cloud ≠ backup
Cloud data	Rely on sync	Cloud backup	Independent backup	IT/ops	Daily	Protect from deletion

Common mistakes

- Back up only My Documents
- Assume emails on the cloud are automatically backed up
- Do not make back ups of accounts payable / receivable or other financial/CRM systems
- Expect that employees will take responsibility for making back up copies of their files

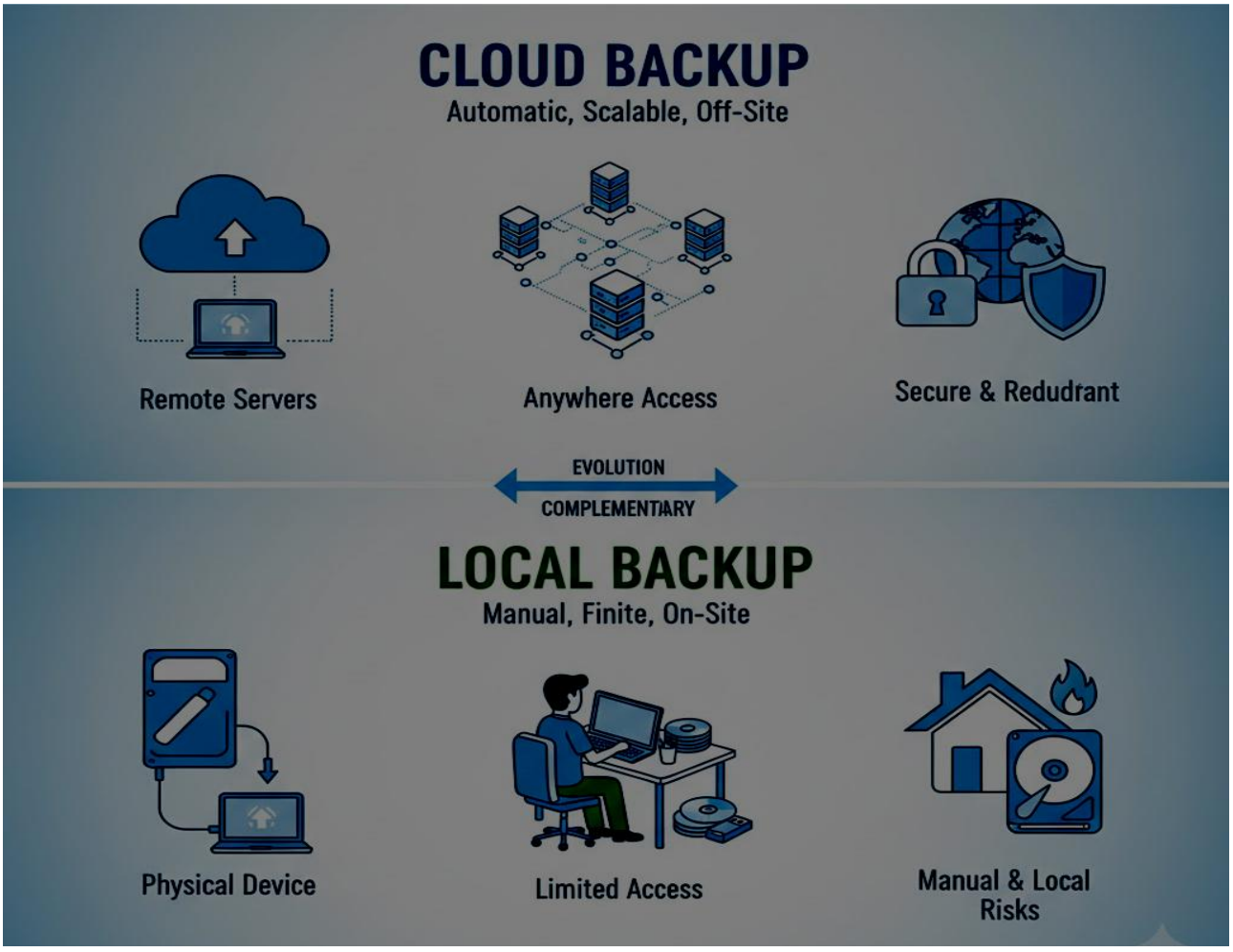
Quick wins

- Identify the types of data you cannot afford to lose and why
- Determine where business-critical applications save their data
- Check whether your business email accounts are being backed up.

2) Backup locations & methods

Why it matters

When you have all your data together in one location, one single incident can wipe out everything, be it fire, theft, ransomware or just a simple system failure.



Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
Local backup	External drive	NAS device	Automated local copy	Office mgr	Daily	Fast restores
Off-site copy	Manual rotation	Cloud backup	Immutable cloud copy	IT/ops	Daily	Critical protection
Separation	Same room	Different building	Different provider	IT/ops	Ongoing	Reduce single points
Immutability	None	Limited	Time-locked backups	IT/ops	Ongoing	Ransomware defence

Common mistakes

- Only using one USB drive as a backup
- Storing the backup alongside the computer
- Not having an offsite backup
- Having the backup accessible 24/7 and writable

Quick wins

- Adding at least one offsite copy of your backup
- Rotating at least one copy of your backup to a location away from the PC
- Using read-only or time-locked backups, if available.

3) Backup frequency & retention

Why it matters

The discovery of data loss usually occurs several days or weeks later. If you don't have a backup that goes back far enough, then it’s essentially useless.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
Backup frequency	Daily	Multiple daily	Continuous for key data	IT/ops	Daily	Automate
Retention	7 days	30 days	90–365 days	IT/ops	Ongoing	Balance cost
Versioning	Latest only	Multiple versions	Long-term versions	IT/ops	Ongoing	Protect from mistakes

Common mistakes

- Last copy kept
- Retention periods are very short
- Retention rules not established in writing

Quick wins

- Establish a minimum 30-day retention period
- Make older versions recoverable

4) Security of backups

Why it matters

If an attacker breaks into the backup, he can encrypt or delete the backups as well.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
Encryption	At rest	At rest + transit	Strong encryption everywhere	IT/ops	Ongoing	GDPR expectation
Access control	Shared login	Limited admins	Separate backup accounts	IT/ops	Ongoing	Least privilege
MFA	Not used	Where possible	Mandatory	IT/ops	Ongoing	Protect admin access
Ransomware	None	Detection	Immutable backups	IT/ops	Ongoing	Key defence

Common mistakes

- Using the same credentials for your backup and system
- No encryption
- There are multiple people with access to it

Quick wins

- Create a separate administrative account dedicated to your backup
- Where applicable, enable multi-factor authentication

5) Monitoring & alerts

Why it matters

If a backup quietly fails to operate properly, it could leave you unprotected for up to 4 weeks.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
Alerts	Manual checks	Email alerts	Dashboard + alerts	IT/ops	Daily	Fail fast
Reviews	Ad hoc	Weekly check	Monthly review	Office mgr	Weekly	Simple log
Reporting	None	Basic reports	Trend monitoring	IT/ops	Monthly	Spot issues

Common mistakes

- Assumed 'Set it & forget it'
- Sending Alert Notifications to Your Former Staff
- No One is Checking Backup Reports

Quick wins

- Implement Failure Alert Notifying System Now
- Delegate Weekly Backup Report Check-Up to One Person

6) Restore testing & verification

Why it matters

Backups have no importance unless you are able to restore from them.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
File restore test	Rare	Annual	Quarterly	Office mgr	Quarterly	Random files
Email restore	Not tested	Occasional	Scheduled test	IT/ops	Quarterly	Older data

Common mistakes

- Testing Restores are not done
- Only recent backups were tested

- Fail to keep documented records

Quick wins

- Select One Test Restore to Perform This Month
- Document Test Restore Results

7) Responsibilities & documentation

Why it matters

If everyone thinks someone else is responsible for backing up, then your backups will fail to operate, or fail to operate as expected.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency	Notes
Backup owner	Informal	Named person	Named + deputy	Director	Ongoing	Accountability
Documentation	None	Basic notes	Clear run-book	Office mgr	Annual	Simple is fine
Incident contact	Unclear	Known internally	Documented	Director	Ongoing	Fast response
Review cycle	None	Annual	Scheduled	Director	Annual	Keep current

Common mistakes

- Server backup responsibility is not assigned to any person
- No written documentation of server backup process
- No one has updated server backup documentation

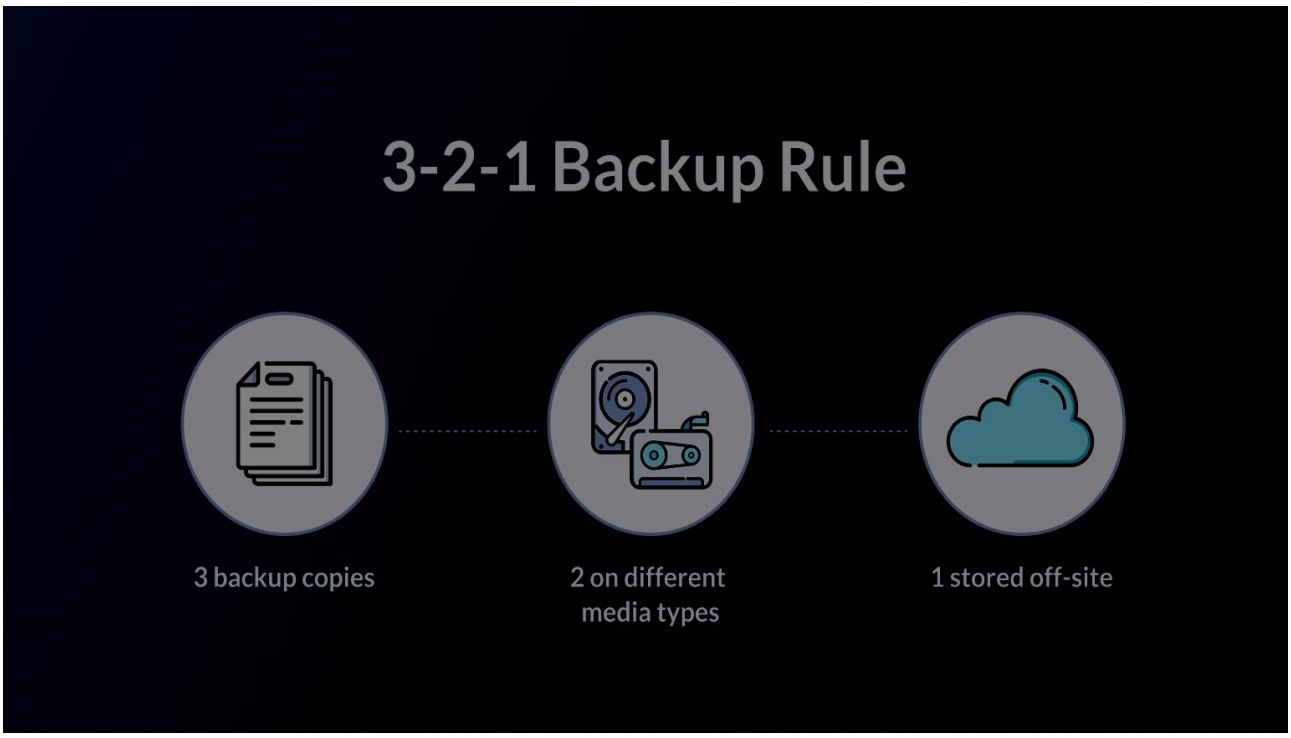
Quick wins

- Assign a server backup owner now
- Write up a 1-Page Summary of Your Server Backup System

The 3-2-1 backup rule

- 3 copies of the data you have.
- 2 different kinds of storages you have.
- 1 copy stored off-site.

For example, the original files stored on a computer, a device used for backing them up locally, and a cloud service where the files are stored in a separate location from the computer.



Cloud services ≠ backups

Many of the current types of cloud storage protect against hardware failure, but they still leave your data vulnerable to:

- Accidental deletion.
- Deliberate (malicious) deletion.
- Ransomware attacks.
- Long-term data recovery.

Due to these vulnerabilities third-party backup solutions are typically required for solutions such as Microsoft 365.

Common backup failures & misconceptions

- "For sure we are covered because we have the cloud"
- "We have never lost any data"
- "The IT Department is responsible for backups"
- "One USB drive is adequate"

Each of these represents an unnecessary risk.

30-day backup setup plan

Week 1	Week 2
❿ Identify the data that is important. ❿ Select an individual as the backup owner. ❿ Determine where the backups will be saved.	❿ Set up automated backups. ❿ Restrict access to backups. ❿ Send notifications when a backup has been created.
Week 3	**Week 4**
❿ Test how to restore the data backed up. ❿ Write down the backup procedures and how to restore them. ❿ Make everyone in the company aware of the backups and how to use them.	❿ Look for any shortcomings in your backup process. ❿ Change your retention periods. ❿ Establish a schedule for regular reviews of your backup process.

FAQs

- **Are backups necessary when using the cloud?**

Yes, the cloud does not provide you with a full backup.

- **How often should I back up my data?**

At least once a day for all data, but more frequently for critical data.

- **How long should I keep backups?**

At least 30 days for most small businesses.

- **What measures are in place to protect against ransomware on backups?**

We use separate access for backups, encrypted data and immutable backup copies.

- **Who is responsible for backups?**

An individual within your company should be named as the backup owner.

- **Does GDPR require backups?**

No, but GDPR does have documents to establish availability and integrity.

- **Can employees make their own backups?**

Yes, but your company will retain ultimate responsibility.

- **What is the cost of backing up?**

Costs vary, but usually the more straightforward the backup, the less expensive it will be.

- **What happens if I am unable to restore my backups?**

Alerts will be sent to you and you should investigate the backup failure immediately.

- **How often should restorations of backed-up data be tested?**

At least every quarter.

About This Guide

The **Computer Support Centre** has created this guide to assist micro and small business owners in the UK in comprehending the concept of backup. It is an easy-to-read resource created specifically for non-technical people such as business owners, office administrators, and business directors. This guide provides simple tips on how business owners can quickly implement a backup system that will protect their company's data without requiring the use of complicated systems or terminology.

This guide focuses on being practical and achievable; it provides information on which data needs to be backed up, the frequency at which backups need to be performed, and how micro and small business owners can reduce the chances of losing their company's data to malicious programs such as ransomware, user error, or hardware failure. It has been created to represent the types of business that are typically found in the UK (small offices) while providing some guidance on compliance with Cyber Essentials and UK GDPR, without offering legal advice.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

Managing backups is not just a technical procedure, it’s essential for any business.

Small businesses are more likely to experience losses caused by accidents (like accidentally deleting files), system failures (such as a hardware issue), or ransomware; they are less likely to be targeted for an advanced attack.

When small businesses implement a systematic approach to backing up their important information, create an assigned point of contact for ongoing management of those backups (for example, the same person that prepares the monthly financials), and conduct regular test restores to verify that their off-site backups actually work — they are able to reduce both the delay to recover and the amount of disruption caused when data is lost.

You should regularly revisit this checklist to reflect how your business is growing, as well as how your systems and staff are changing and adapting flexibly. Establishing a basic, but properly maintained backup plan provides an excellent way to prevent disruption in your daily business.