Alternative Provision – Cyber Threat Readiness & Response Checklist

Updated: 01 May 2026 • Owner: Churchwood CIC • Review cycle: Termly

How to use this checklist: Review each item, mark ☑ when complete, add owners and due dates. Keep this with your safeguarding, business continuity, and data protection packs.

1) Governance & Roles

- ☑ Named Senior Responsible Officer (SRO) for cyber security is appointed and documented (e.g., Provision Lead/DSL).
- ☑ Cyber risk is on the organisation risk register with termly review.
- ☑ Data Processing Agreements in place with the Local Authority (LA) and all processors/suppliers.

2) Identify & Asset Management

- ☑ Up-to-date inventory of all devices (staff, young person, loan), servers, network kit, and cloud services (MIS, safeguarding, email, file storage).
- ☑ Critical systems identified with designated owners and RTO/RPO set (Recovery Time/Point Objectives).
- ☑ Admin accounts identified; use is restricted and monitored.
- ☑ Third-party integrations mapped (LA systems, MIS, safeguarding tools, payment platforms).

3) Protect – Technical Controls

- ☑ MFA enforced for staff email, admin consoles, MIS, safeguarding and remote access.
- ☑ Automatic updates/patching enabled on OS, apps, network devices; legacy/unsupported systems removed or isolated.

- ☑ Reputable endpoint protection/EDR deployed and centrally managed.
- ☑ Email security in place (anti-phish, DMARC, SPF, DKIM) and attachment sandboxing where available.
- ☑ Least-privilege access and role-based permissions reviewed at least termly.
- ☑ Secure configuration baseline applied (BitLocker/FileVault, firewall enabled, USB controls as appropriate).
- ☑ Strong password policy in place (length, reuse limits) and password manager available to staff.
- ☑ Network segmentation for admin/guest/pupil; Wi-Fi secured with strong authentication.
- ☑ Encryption at rest and in transit for sensitive data (incl. portable devices).

4) Protect – People & Process

- ☑ Induction and annual refresher training covering phishing, social engineering, data handling, and reporting routes.
- ☑ Regular phishing simulations with feedback (no blame).
- ☑ Clear Joiners-Movers-Leavers process (account creation, privilege review, timely deprovisioning).
- ☑ Visitor and contractor access controlled; admin access never shared.

5) Detect & Monitor

- ☑ Central log collection enabled for key systems (email, identity, MIS, safeguarding, firewall).
- ☑ Alerts configured for suspicious sign-ins, MFA failures, mass file deletion, mailbox rules, privilege escalation.
- ☑ Dark web and credential exposure monitoring in place (where feasible).
- ☑ CCTV and physical access logs retained and reviewable (where relevant to incidents).

6) Backup & Recovery

- ☑ Backups follow 3-2-1 rule (at least one offline/immutable) for MIS, file shares, safeguarding data.
- ☑ Backups are encrypted, tested through termly restore drills, and documented.
- ☑ Clear offline contact method and printed recovery steps available for 'no-IT' scenarios.

7) Incident Response – Playbook

- ☑ Single reporting route for suspected cyber incidents (email/phone/teams chat) with 24/7 escalation method.
- ☑ Triage guide defines severity levels and first actions (isolate device, change passwords, preserve evidence).
- ☑ Pre-agreed external support: LA IT/security, vendor support, insurer/broker, legal counsel, police (as needed).
- ☑ Evidence handling and chain-of-custody notes template prepared.
- ☑ Template announcements for staff, parents/carers, and commissioners prepared in advance.

8) Legal, Safeguarding & Regulatory

- ☑ Data breach assessment process in place (UK GDPR Art. 33/34) with 72-hour ICO reporting decision workflow.
- ☑ Safeguarding pathway considered for cyber incidents involving pupils (DSL, MASH, police as appropriate).
- ☑ Records of processing and DPIAs include cyber risk controls (esp. high-risk/special category data).
- ☑ Insurance reviewed for cyber coverage and incident response services.

9) Supplier & Cloud Security

- ☑ Due diligence completed for key suppliers (MIS, filtering, safeguarding, comms, payments).
- ☑ Contractual security clauses and incident notification SLAs verified; sub-processors listed.
- ☑ Access to AP data by suppliers uses MFA, logging, and least privilege.
- ☑ Exit plans defined (data export, secure deletion, handover with LA).

10) Testing & Continuous Improvement

- ☑ Termly tabletop exercise of a realistic scenario (e.g., ransomware or email compromise) with lessons logged.
- ☑ Annual technical test (e.g., external vulnerability scan or penetration test) and remediation tracked.
- ☑ Metrics reported to leadership: phishing-click rate, patch latency, unresolved high-risk findings.

Annex A – Rapid Incident Log (use during an event)

Time	Action / Event	Owner	Notes

This checklist aligns with good practice for UK schools/APs and complements safeguarding, data protection, and business continuity arrangements.