Bedford Greenacre Independent School

# Annual Cyber Risk Assessment and Cyber Awareness Plan (ISI Compliant)

## 1. Governance & Role Allocation

**Strategic Oversight:** Principal (Ian Daniel – ID)

Overall accountability for cyber security and data protection.

- Reports cyber risk to Governors
- Signs off:
    - Annual cyber risk assessment
    - Incident reports (serious breaches)
- Ensures alignment with safeguarding culture

**Safeguarding Oversight:** Designated Safeguarding Lead (Emma Brewer – EB)

- Ensures cyber risks impacting pupil safety are identified
- Oversees:
    - Safeguarding system security
    - Online safety risks (cyberbullying, grooming, data exposure)
- Involved in all incidents involving pupil data or safeguarding concerns
- Links cyber risks to KCSIE compliance

**Operational Cyber Management:** IT Technician (Mike Sorbo – MS)

- Leads technical implementation of controls
- Responsible for:
    - Network security
    - Antivirus / firewall / patching
    - Backup systems
    - User account security
- Maintains cyber risk register (operational level)

**Data Protection & Compliance:** Business Manager (Sue Diffey – SD)

- Oversees:
    - GDPR compliance
    - Data protection policies
    - Third-party supplier risk

- Approves:
    - DPIAs for new systems
- Works with IT Lead on:
    - Financial system protection
    - Cyber fraud prevention

**Departmental Responsibility:** Heads of Department / Admin Staff

- Ensure:
    - Safe handling of pupil data
    - Compliance with password and email protocols
- Act as first line of defence

**All Staff**

- Responsible for:
    - Following cyber policies
    - Reporting incidents immediately
    - Completing annual training

## 2. Bedford Greenacre School Cyber Risk Register (Core Risks)

### A. Safeguarding System Breach

- Owner: EB / MS
- Risk: Unauthorised access to safeguarding records
- Controls:
    - Restricted access (DSL team only)
    - MFA enabled
    - Audit logs

### B. Phishing / Email Compromise

- Owner: MS / ID (awareness culture)
- Risk: Staff disclose credentials or click malicious links
- Controls:
    - Email filtering system
    - Staff awareness training
    - Financial verification procedures

**C. Management Information System (MIS) / Pupil Data Breach**

- Owner: SD / MS
- Risk: Exposure of pupil/staff data
- Controls:
    - Role-based permissions
    - Encryption
    - Secure backups

**D. Financial Fraud (Invoice Scams)**

- Owner: SD
- Risk: Fraudulent payment requests
- Controls:
    - Call-back verification for bank changes
    - Dual authorisation for payments

**E. Device Loss or Theft**

- Owner: MS
- Risk: Data loss via laptops or mobile devices
- Controls:
    - Device encryption
    - Remote wipe
    - Password lock policies

**F. Third-Party Software Risk**

- Owner: SD / MS
- Risk: External platform data misuse
- Controls:
    - Supplier due diligence
    - Annual review

**G. Ransomware / System Failure**

- Owner: ID / MS
- Risk: School operations disruption
- Controls:
    - Daily offsite backups
    - Disaster recovery plan
    - Incident response plan

## 3. Annual Cyber Risk Assessment Cycle

**Autumn Term (Primary Review)**

Led by: MS/SD/EB

- Output:
    - Updated risk register
    - Control review
    - Staff training plan

**Spring Term (Assurance Check)**

- Phishing test MS
- DSL review of safeguarding risks
- Report to Principal

**Summer Term (Formal Reporting)**

- Principal reports to Governors:
    - Risk status
    - Incidents (if any)
    - Training compliance

## 4. Cyber Awareness Plan (Role-Specific)

All Staff (Mandatory Annual Training)

Delivered by: IT Lead / external provider
Content:

- Phishing awareness
- Password security
- Data protection (GDPR)
- Safeguarding link (critical for ISI)

**Record kept for inspection**

DSL & Safeguarding Team

Additional focus:

- Data breach handling
- Online safety risks
- Cyber incidents involving pupils

**SD & Finance Team**

High-risk group – enhanced training:

- Invoice fraud awareness
- Payment verification procedures
- Email spoofing risks

**Senior Leadership Team (Including Principal)**

Focus on:

- Incident leadership
- Decision-making during breach
- Communication management

**Pupils (Curriculum-Based)**

Led by: EB / Computing / PSHE

Content:

- Online safety
- Cyberbullying
- Responsible device use

**Parents**

- Annual communication issued
- Optional workshop / guidance:
    - Device safety
    - Social media risks

## 5. Incident Response Structure (Bedford Greenacre Model)

**Step 1: Immediate Reporting**

Any staff → MS + EB

**Step 2: Initial Assessment**

- MS → technical containment
  EB → safeguarding impact

**Step 3: Escalation**

- Serious incidents reported to:
    - Principal (ID)
    - Business Manager (SD)

**Step 4: External Reporting (if required)**

- ICO (data breach)
- Police (serious fraud/crime)

**Step 5: Review**

- Logged and reviewed in:
    - Safeguarding records (if relevant)
    - Risk register

**6. Evidence for ISI Inspection**

You should be ready to show:

- Annual cyber risk assessment (this document)
- Named roles and responsibilities (clear governance)
- Staff training logs Incident log (even if nil return)

Evidence of:

- DSL involvement
- Governor oversight
- Safeguarding linkage

**7. Key ISI Inspection Strength (High Impact)**

- To align with current inspection focus (based on trends in safeguarding findings)
- Explicitly linking cyber security to safeguarding is critical

Make sure:

- DSL is clearly involved
- Cyber risks appear in safeguarding discussions
- Staff understand "cyber = safeguarding"