Safeguarding Checklist

A. Safeguarding Leadership & Accountability

☐ Designated Safeguarding Lead identified and contact details available

☐ All staff trained and aware of safeguarding responsibilities

☐ Clear reporting routes for safeguarding concerns

☐ Confidentiality rules understood by all staff

B. Technology & Online Safety Controls

☐ E-Safety policy is in place, reviewed annually, and communicated to all staff

☐ Acceptable use rules defined for:

- Social media
- Mobile devices
- Digital communication tools

☐ Online behaviour rules for staff and students understood

☐ Filtering & monitoring in place (firewalls, content filtering, logging)

C. MIS, Telephony & Communication Safeguards

☐ MIS data accuracy checked regularly

☐ Staff know how to rapidly access contact details (important in emergencies)

☐ Safeguarding call flows configured (e.g., escalation groups, DSL contact routing)

☐ Call recording enabled for safeguarding-related calls

☐ Lockdown alerts configured and tested

D. Reporting & Incident Management

☐ Clear process for reporting:

- Safeguarding concerns
- Online abuse or suspicious behaviour
- Breaches of acceptable use terms

☐ Evidence logs maintained securely

E. Data Protection & Privacy

☐ Staff trained on data-handling (GDPR, secure files, access control)

☐ Devices protected with MFA, strong passwords, encryption where applicable

☐ Secure remote access procedures in place

F. Review & Audit

☐ Safeguarding & E-Safety policies reviewed annually

☐ Technology safeguarding processes tested termly

☐ Lessons learned captured and implemented