

Cyber-Security Risk Assessment

Clarity Independent School, Woodhill Road, Sandon CM2 7SG

Date of Assessment: 17th July 2026

Assessed by: GL and MD

Next Review Date: December 2026

Severity	Multiplier								Key	
Extreme / Catastrophic	5	5	10	15	20	25		Severe	20 - 25	Unacceptable level of risk exposure which requires immediate corrective action to be taken
Major	4	4	8	12	16	20		Major	12 - 16	Unacceptable level of risk exposure which requires constant active monitoring, and measures to be put in place to reduce exposure
Moderate	3	3	6	9	12	15		Moderate	5 - 10	Acceptable level of risk exposure subject to regular active monitoring measures
Minor	2	2	4	6	8	10		Minor	3 - 4	Acceptable level of risk exposure subject to regular passive monitoring measures
Insignificant	1	1	2	3	4	5		Insignificant	1 - 2	Acceptable level of risk subject to periodic passive monitoring measures
Multiplier		1	2	3	4	5				
Likelihood		Remote	Unlikely	Possible	Possible	Certain				

1. Scope

This assessment covers cyber risks relating to:

- Pupil data
- Staff data
- Safeguarding and welfare records
- School financial systems
- Devices and network access
- Online learning platforms
- Email and communication systems

2. Key Risks and Controls

Risk	Impact	Likelihood	Control Measures	Further Action
Unauthorised access to sensitive pupil/staff data	Moderate / major - GDPR breach, safeguarding risk	Possible	- Strong password policy - 2-factor authentication - Limited access based on role - Staff and pupils e-safety agreement prior to use	Annual audit of permissions Regular staff training
Phishing emails or malicious links	Moderate / major - data theft or ransomware	Possible	- Email filtering - Phishing training (ICO cyber training) - Reporting system - Staff and pupils e-safety agreement prior to use	Termly refresher training Simulated tests
Loss or theft of school devices	Moderate / major - data confidentiality risk	Possible	- Device encryption - Remote wipe / 'findmydevice' - Usage policy	Termly asset register review Immediate reporting of lost devices by staff

			- All documents stored on G drive / icloud – password protected - Staff and pupils e-safety agreement prior to use	
Insecure remote access	Moderate / major - external breaches	Possible	- Secure VPN/cloud platform - Admin rights limited - No personal device access unless 2 factor authentication - Staff and pupils e-safety agreement prior to use	Quarterly security test
Inappropriate online content access by pupils	Minor / moderate – safeguarding concern	Possible	- Filtering software - Supervision - Digital safety lessons - Staff and pupils e-safety agreement prior to use - Pupil supervision on computers - No access to mobile devices at school	Monitoring reports Parent engagement
Outdated software and systems	Moderate / major - vulnerable to exploits	Possible	- Regular updates - Supported software only	Staff required to notify Main Office if they wish to subscribe
Poor staff cyber hygiene	Moderate / major	Possible	- Code of Conduct - Best practice training - No password sharing - Staff and pupils e-safety agreement prior to use	Staff reminders and induction
Ransomware or	Major - system/data	Unlikely-	- Antivirus	Annual plan review

malware attack	disruption	Possible	- Automatic, secure backups - Incident response plan	
Cyberbullying or online misconduct	Moderate / major - emotional impact	Possible	- Online safety policy - Clear expectations taught - Incidents dealt with learning consequences - Supervised access - Staff and pupils e-safety agreement prior to use	Include in curriculum

3. Roles and Responsibilities

- Headteacher: Oversees cyber strategy and safeguarding
- DSL: E-safety Lead and safeguarding lead
- DPO: Ensures GDPR compliance and breach response
- IT Support Provider (Danny Lagden): Maintains security and supports incident response
- All Staff: Follow good practice and report incidents
- All pupils: Follow good practice, report incidents, work with school staff to keep each other safe

4. Training and Awareness

- Staff receive cyber safety training annually (ICO Cyber Security and Educare Online Safety)
- Pupils receive digital safety education through PSHE and ICT lessons
- Parents receive half-termly online safety update newsletters

5. Incident Response

In the event of a cyber incident – follow procedure in E-safety policy and...:

- Report immediately to Headteacher, DSL and IT support
- Isolate affected systems
- Notify DPO and follow breach response
- Notify ICO if required

6. Review and Update

This risk assessment will be reviewed annually or after a cyber incident/near miss.

7. Action Plan 2025 – 2026:

Action Required	Responsible Person/Role	Deadline/Review Frequency			
		Half-termly	Termly	Annually July	As incidents occur
Audit and update user access permissions across systems	DPO / HT / IT Support			Y	After staff changes
Deliver phishing awareness training to all staff	Headteacher / DSL		Y		
Ensure encryption and remote wipe are active on all mobile devices	IT Support		Y		
Review remote access security settings	IT Support		Y (DL)		

Maintain filtering and monitoring software for pupil internet use	IT Support / DSL	See filtering log			
Update all software and operating systems regularly	IT Support				Y auto-updates as used
Reinforce staff training on password security and data handling	Headteacher			Y – annual training	Y – staff induction
Test and review incident response plan for cyber attacks	Headteacher / DPO			Y – policy update	
Integrate digital safety into PSHE and Computing curriculum	SENDCo / Teachers		Y PSHE ICT curriculum		
Send online safety updates to parents	Headteacher / DSL	Y			
Maintain asset register for school devices	Business Manager / IT Support			Y – PAT testing Sept	
Check hard drive of all devices annually	Business Manager / IT Support			Y	
Log and investigate any cyber incidents or near misses	Headteacher / DPO / DSL				Y