# Cyber Security Policy

## Clarity Independent School

**Bridge Barn Farm**
**Woodhill Road**
**Sandon**
**CM2 7SG**

**Clarity Independent School is committed to safeguarding...**

*"Our school is committed to our whole-school approach to safeguarding, which ensures that keeping children safe is at the heart of everything we do, and underpins all systems, processes and policies...We promote an environment where children and young people feel empowered to raise concerns and report incidents and we work hard in partnership with pupils, parents and caregivers to keep children safe."*

Clarity Safeguarding Policy September 2025

**Written by Richard Clow**

**This is version [1.1]**
**Written:** September 2025
**Mid-Year Update:** November 2025 for September 2025
**Updated by Name:**

## 1. Introduction

Clarity Independent School is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and latest Keeping Children Safe in Education guidance.

## 2. Scope

This policy applies to all staff, students, and any third parties who have access to Clarity Independent School's IT systems and data.

## 3. Roles and Responsibilities

| **Role** | **Responsibilities** |
|---|---|
| Head of Centre | **Debbie Hanson** to oversee policy updates and ensure compliance with JCQ Regulations. |
| IT Business Manager | **Grace Hanson** to monitor systems, respond to incidents, manage access and updates, liaison with the school's IT support from D L Solutions, DLS Computers Ltd. |
| Data Protection Officer | **Grace Hanson** to ensure compliance with data protection law, advise on data handling, and oversee data breaches. |
| Exams Officer | **Richard Clow** to ensure that logins for exam use laptops are kept secure and that laptops are set up according to the JCQ Instructions for Conducting Examinations 2025/26 (ICE) Regulations, ensure that storage devices used for live exams are stored in the secure storage facility until despatched for moderation. |
| DSL and Quality Nominee | **Michelle Deveney** to ensure that school e-safety procedures comply with cyber security policies and latest Keeping Children Safe in Education regulations. |

| Role | Responsibilities |
|---|---|
| All Staff | Follow this policy, complete annual training through the NCSC, report incidents or concerns promptly within the centre. |
| Students/Users | Use IT systems responsibly according to the ICT agreement and report any concerns to staff. |

## 4. Technical Security Measures

Clarity Independent School implements the following security measures, scaled to our size and needs:

- Firewalls and network security controls
- Anti-virus and anti-malware software on all devices
- Regular software updates and patch management
- Secure data backup and tested recovery procedures
- Encryption for sensitive and personal data
- Multi-factor authentication (MFA) for critical systems and remote access
- Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace)
- Prompt removal of access for leavers

## 5. User Account Management

Password governance must follow NCSC Guidance:

  - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
  - https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

- Access control and permissions are based on job roles and reviewed regularly.
- Accounts are promptly disabled when users leave.
- Account activity is monitored and audited.

## 6. Staff Training and Awareness

All staff must complete annual cyber security training and annual refresher training to include:

- Phishing awareness and social engineering defence training
- Whole staff E-safety training delivered by the DSL / Educare online
- Annual training using the NCSC schools training pack.

- https://www.ncsc.gov.uk/information/cyber-security-training-schools
- Exams Office Cyber Security: Account Management Best Practices. (Exams staff only).

Records of cyber training must be retained for all staff and be available for inspection.

## 7. Incident Response Plan

All staff members must report any suspected security incidents or concerns to **Debbie Hanson, Head of Centre,** immediately using the following procedures:

- Steps for identifying and reporting incidents using the Whistleblowing Policy procedures and safeguarding procedures by alerting the DSL or DDSL's.
- An incident response team will then be composed by the Head of Centre
- Communication plan for stakeholders: Informing awarding bodies and JCQ Inspections Team of security or potential security breaches as instructed by awarding bodies and JCQ Regulations procedures, informing IT support, reporting the incident to the NCSC.
- Conduct a post-incident review process to identify lessons learned and update procedures if necessary, including updating the Cyber Security Policy, Contingency Policy and Plan and other related policies.

## 8. Compliance and Auditing

Cyber security needs to constantly evolve to meet the ever-changing threats posed by criminals. Clarity Independent School will ensure that this is met by holding:

- Regular internal audits: (see our Cyber Security Risk Assessment and Action Plan)
- External audits:  DL Solutions

## 9. Policy Review

This policy will be reviewed annually by a member of the Senior Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.

Overall responsibility for the Cyber Security Policy in **Clarity Independent School** rests with the Head Teacher, Debbie Hanson.