Chace Community School

Cyber Security Policy (Exams)

2025/26

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Tanya Douglas/Carly Lynch/Julie Marshall/ Justin Wing	
Date of next review	October 2026

Key staff involved in the policy

Role	Name(s)
Head of centre	Tanya Douglas
Senior leader(s)	Krysia Sosin, Natalie Slade, Alex Greig, Barbara Terziyski, Carly Lynch, Amanda Roper, Gamze Sahin
IT manager	Justin Wing
Data, Assessment and Systems Manager	Julie Marshall

1. Introduction
Chace Community 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 Keeping Children Safe in Education guidance.

2. Scope
This policy applies to all staff, students, governors, and any third parties who have access to Chace Community's IT systems and data.

3. Roles and Responsibilities

Role	**Responsibilities**
Head of Centre	*Overall responsibility for policy implementation and cyber security strategy.*
IT Manager/Team	Justin Wing to *implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer	Julie Marshall to *ensure compliance with data protection law, advise on data handling, and oversee data breaches.*
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures
Chace Community 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 which includes:
  - The importance of creating strong, unique passwords for all accounts
  - Keeping all account details strictly confidential
  - The critical role of Multi-factor Authentication (MFA) in protecting against unauthorised access.
  - The importance of staff quickly reporting any suspicious activity, events, incidents and encouraging a safe and supportive reporting culture
  - Phishing awareness and social engineering defence training.

https://www.ncsc.gov.uk/section/education-skills/cyber-security-Centres#section_1**7.**

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

7. Incident Response Plan

- Steps for identifying and reporting incidents: All staff members must report any suspected security incidents or concerns to Julie Marshall immediately.
- Incident response team:

	Name	Role in School
Recovery Team Leader	Justin Wing / Julie Marshall	Network Manager/Data Manager
Data Management	Justin Wing / Julie Marshall	Network Manager/Data Manager
IT Restore / Recover	Roger Davies	IT Operation Manager
Site Security	Sean Spink/Sunalp Emir	Site Managers
Public Relations	Gina Panayi	Head Teachers PA
Communications	Gina Panayi	Head Teachers PA
Resources / Supplies	Simone Fernandez	School Business Manager
Facilities Manage		Site Manager

- Communication plan for stakeholders:
    - Enact your Cyber Recovery Plan
    - Contact the 24/7/365 RPA Cyber Emergency Assistance:
    - By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**
    - You will receive a guaranteed response within 15 minutes
    - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible
    - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
    - Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
    - Contact your local police via Action Fraud Action Fraud website or call **0300 123 2040**
    - Contact the Local Authority (LA)
    - Contact your Data Protection Officer
    - Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 111**
    - Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk
- Referral to awarding organisation(s)
- Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary led by Julie Marshall.

8. Compliance and Auditing

- Annual review and update of this policy
- Regular internal audits:Termly

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.
- This policy will be ratified by: Senior Leadership Team