IT & Cyber Security Policy

The Rushmere Academy

Rushmere

'Inspiring change'

September 2025

PERSON RESPONSIBLE FOR POLICY:	***MICHELLE HARVEY***
APPROVED:	***GABRIELLE BARTON***
SIGNED:	***MICHELLE HARVEY*** ***GABRIELLE BARTON***
TO BE REVIEWED:	***SEPTEMBER 2026***

UKPRN: 10044130 | Legal Address: 20 Francis Street, Northampton, NN1 2NZ

Tel: 01604 635586 / 07729090459

1) Purpose & Scope

This policy sets out how we keep learners, staff and data safe when using technology. It applies to all staff, contractors, volunteers, governors/directors, learners and visitors using our devices, systems or data on-site or remotely. It covers our Microsoft/Google platforms, on-site equipment, and any cloud services we use.

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, education providers need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole.

Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

2) Roles & Responsibilities

- Directors: ensure appropriate resources, oversight and approvals.
- Managing e-safety and embedding it throughout the Centre.
- Centre Coordinator: accountable for meeting standards and resourcing.
- Designated Safeguarding Lead (DSL): links online safety alerts to safeguarding procedures.
- Data Protection Officer (DPO): advises on data protection and breach response.
- IT Support (Simply IT – Managed Service Provider): implements technical controls, reports risks, and supports staff.
- All Users: follow this policy and our Acceptable Use Policies (AUPs).
- Personal mobile telephones – see Safeguarding and child protection policy.

2a) Cyber safety in the Curriculum

Rushmere Academy provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that maybe encountered outside education is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Learners are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Learners know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

2b) Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the website.

This consent form is considered valid for the entire period that the child attends the provision unless there is a change in the child's circumstances where consent could be an issue.

Pupils' names will not be published alongside their image and vice versa on the website, x account, mobile app or any other Rushmere based publicity materials.

2c) SEND

Rushmere endeavours to deliver a consistent message to parents and pupils with regard to the cyber rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of cyber issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.
Internet activities are planned and well-managed for these children and young people

3) Standards We Follow

- UK GDPR & Data Protection Act 2018 (72-hour breach notification where required).
- DfE Filtering & Monitoring standards (used as a benchmark).
- NCSC cyber security good practice (MFA, patching, backups).

4) Key Controls

A. Accounts & Access

- Least-privilege access; joiners/movers/leavers handled promptly.
- Multi-Factor Authentication (MFA) on admin, remote access and cloud platforms where available.
- Strong passphrases (three or more random words); password manager for staff; admin and standard accounts kept separate.

B. Devices & Updates

- All devices recorded and encrypted (BitLocker/FileVault). Auto-lock enabled.
- Apply security updates within 14 days for High/Critical risks (aim sooner).
- Anti-malware enabled on all endpoints and servers.

C. Network, Filtering & Monitoring

- Firewalls on all devices or at the boundary; sensible network segmentation.
- Appropriate filtering and monitoring in place; alerts reviewed and actioned with a clear escalation route to the DSL where safeguarding is indicated.

D. Backups & Continuity

- 3-2-1 backups for key systems (MIS, file data, platforms).
- Restore tests carried out at least once per term; RPO/RTO recorded.

E. Cloud & Suppliers

- Maintain a register of systems and processors (data location, retention, and exit plan).
- Ensure contracts include data-processing terms; review key suppliers annually.

F. Data Handling

- Use approved storage only; no sensitive data in personal email or unapproved apps.
- Encrypt data in transit and at rest where supported.

5) Incident Response & Reporting

All suspected security events should be reported immediately to Simply IT and the DSL where safeguarding is involved. Incidents are recorded, contained, investigated and lessons learned. If personal data is involved, the DPO assesses risk and the ICO is notified within 72 hours where required; affected individuals are informed when the risk is high.

6) Training & Awareness

- Annual cyber training for staff (with refreshers after incidents).
- Age-appropriate online-safety education for learners.
- Induction for volunteers/visitors where relevant.

7) Review

Directors approve this policy annually. A termly review note and action plan will be updated by the SLT digital lead and Simply IT.

Sign-off

- Policy Owner (Head/Principal): ____________________________ Date: ___________
- DSL: ____ Date: ___________
- DPO: ____ Date: ___________
- Simply IT (MSP) Representative: __________________________ Date: ___________

Compliance Position

We are not a registered school or college, so Keeping Children Safe in Education (KCSIE) is not statutory for us. We align to KCSIE where relevant and proportionate, and we follow the Department for Education Out-of-School Settings (OOSS) guidance and the statutory 'Working Together to Safeguard Children', alongside UK GDPR and data-protection law.