Online E Safety Policy

Formally adopted by the Governing Body of:	**Redcastle Family School**
On:	
Adopted by the Governing Body	
Last updated:	**September 2006**

1. Purpose and scope

This policy sets out Redcastle Family School's approach to keeping pupils, staff and the wider school community safe when using digital technologies. It applies to all users of school systems and devices, including staff, governors, volunteers, pupils, parents/carers, contractors and visitors, whether accessing school systems on site or remotely.

The policy aims to:

- Protect pupils and staff from online harm and reduce risks arising from **content**, **contact** and **conduct**.
- Set clear expectations for acceptable and professional use of technology.
- Provide robust procedures for reporting, recording and responding to online safety incidents.
- Ensure compliance with statutory safeguarding guidance, data protection law and recognised cyber security guidance.

2. Key principles

- **Safeguarding first:** Online safety is integral to safeguarding. Staff must follow safeguarding procedures and report concerns immediately.
- **Prevention and education:** We prioritise teaching pupils digital resilience, critical thinking and safe behaviours.
- **Proportionate technical controls:** Filtering and monitoring are used to reduce risk while enabling legitimate educational access. Controls are reviewed and auditable.
- **Clear accountability:** Roles and responsibilities are defined and resourced. Incidents are logged, reviewed and used to improve practice.
- **Partnership with parents:** We work with families to reinforce safe behaviours at home and during remote learning.

3. Governance and responsibilities

Governing Body

- Approve and review this policy at least annually and after significant incidents.
- Ensure sufficient resources for technical controls, training and incident response.

Headteacher

- Implement the policy and ensure staff, pupils and parents are aware of expectations.
- Ensure risk assessments and arrangements for remote learning are in place.

Designated Safeguarding Lead (DSL)

- Lead on online safety incidents and safeguarding concerns; ensure incidents are logged and escalated appropriately.
- Liaise with external agencies (CEOP, Police, LA) and ensure child protection plans remain effective during remote learning.

Data Protection Officer (DPO)

- Provide advice on GDPR and data protection, review third-party contracts and data processing agreements.

ICT Lead / Technicians

- Maintain secure, resilient systems; apply security patches and antivirus updates; manage filtering and monitoring; provide termly reports to SLT and governors.

SENCO

- Ensure pupils with SEND have equitable access and appropriate support for online learning.

All staff

- Model safe, professional online behaviour; complete required training; report concerns to the DSL; use only school-approved platforms and accounts for school business.

Parents / Carers

- Support the school's online safety expectations at home; apply age-appropriate parental controls; report concerns to the school.

Pupils

- Follow the pupil ICT Code of Conduct; report anything that makes them uncomfortable or worried.

4. Education and curriculum (detailed)

- **Progressive curriculum:** Online safety is taught progressively through Computing, PSHE and other subjects. Key strands include: online relationships and respectful behaviour; privacy and personal data; digital footprint and reputation; cyberbullying and reporting; recognising grooming and exploitation; misinformation and source evaluation; copyright and plagiarism; and cyber hygiene.

- **Age-appropriate content:** Lessons and resources are tailored to pupils' developmental stage and reviewed regularly.
- **Active learning:** Use scenarios, role-play, assemblies, peer mentoring and practical activities to build resilience and reporting confidence.
- **Assessment and evidence:** Online safety learning outcomes are assessed and recorded; evidence informs curriculum planning.
- **Staff CPD:** All staff receive induction training on online safety and annual refresher training; additional role-specific training is provided for DSLs, SENCO, ICT staff and senior leaders. Training records are maintained.

5. Acceptable use, accounts and authentication

- **Staff accounts:** Staff must use school-managed accounts for all school business; personal and professional accounts must be kept separate. Multi-factor authentication (MFA) must be enabled where available. Passwords must be strong, unique and changed in line with the school's password policy.
- **Pupil accounts:** Pupils use school-provisioned accounts under supervision and must follow the pupil ICT Code of Conduct. Passwords must not be shared.
- **Guest and contractor access:** Temporary accounts for visitors or contractors are time-limited and monitored.
- **BYOD (Bring Your Own Device):** BYOD is permitted only under the school's BYOD guidance. Personal devices must meet minimum security requirements and must not be used to store protect-level data. The school reserves the right to restrict or block personal devices on the network.

6. Filtering, monitoring and cyber security

- **Filtering and monitoring:** The school operates age-appropriate filtering and monitoring across networks and devices. Settings are reviewed termly, risk-assessed and recorded. Changes to filtering/monitoring are documented and reported to governors.
- **Technical security:** All school devices run approved antivirus software and receive regular security updates. The ICT team performs vulnerability scans and stress testing of remote learning platforms.
- **Network security:** School networks are segmented where appropriate; guest networks are isolated from core systems. Remote access to school systems is controlled and logged.
- **Incident prevention:** Phishing simulations, cyber hygiene training and secure configuration of services are used to reduce risk.

7. Remote learning and live lessons (detailed)

- **Platform approval:** Only school-approved platforms may be used for live or recorded lessons. The ICT Lead maintains an approved platforms list and a configuration checklist.

- **Secure configuration:** Staff must follow NCSC guidance when configuring video conferencing: use waiting rooms/lobbies, meeting passwords, host controls, disable file transfer where appropriate, and restrict screen sharing to hosts. MFA should be enabled for staff accounts.
- **Professional conduct:** Live lessons must be delivered from a suitable, neutral area; staff should use school accounts and, where possible, school-managed devices. One-to-one live sessions are not permitted unless pre-approved and with appropriate safeguarding measures in place (e.g., two-adult rule, parental consent, recording and logging).
- **Pupil expectations:** Pupils must join lessons from a shared family space, wear appropriate clothing, and follow the remote learning code of conduct. Private areas (bedrooms) are discouraged as the primary location for live lessons.
- **Recording and storage:** Recording lessons is permitted only with prior approval and in line with data protection requirements; recordings must be stored securely on school systems and retained only for the agreed period.

8. Data protection and third-party services

- **Due diligence:** Before adopting any third-party service, staff must consult the DPO to confirm GDPR compliance, review privacy notices and sign data processing agreements where required.
- **Protect-level data:** Protect-level or special category data must not be transferred by unencrypted email or insecure methods. Approved secure file transfer solutions must be used.
- **Data minimisation:** Only the minimum personal data necessary for the educational purpose should be collected and processed. Retention schedules must be followed.

9. Reporting, incident management and escalation (detailed)

- **Reporting routes:** Pupils and staff must report online safety concerns to the DSL immediately. Parents should report concerns to the school via the usual channels.
- **Incident logging:** All incidents are recorded centrally using the school's incident log template. Logs must include: date/time, people involved, nature of incident, actions taken, outcomes and any external referrals. Logs are retained for governance and audit.
- **Triage and response:** The DSL will triage incidents, take immediate safeguarding actions where required, and escalate to external agencies (CEOP, Police, LA) for suspected criminal activity or serious harm. The school will refer suspected illegal material to the Internet Watch Foundation and Police without delay.
- **Communication:** The school will inform parents/carers of incidents affecting their children, unless doing so would place the child at further risk. Communications will be factual, timely and proportionate.

- **Post-incident review:** Significant incidents will trigger a review to identify lessons learned and update policies, training or technical controls as needed.

10. Cyber hygiene and phishing

- **User responsibilities:** All users must follow cyber hygiene practices: use strong passwords, enable MFA, install updates promptly, and report suspicious emails or messages.
- **Phishing response:** Suspected phishing attempts must be reported to the ICT team immediately. Staff must not click suspicious links or open unexpected attachments. The ICT team will investigate and, where necessary, block malicious senders and inform users.
- **Backups and recovery:** Critical systems and data are backed up regularly; recovery procedures are tested periodically to ensure resilience.

11. Social media, photography and communications

- **Staff conduct:** Staff must keep professional and personal communications separate. Staff must not accept current pupils as friends/followers on personal social media accounts. School social media accounts must be managed by authorised staff and follow the Staff ICT Code of Conduct.
- **Pupil images:** Parental consent is obtained for use of pupil images. Photographs published online will not include full names and file names/tags will not contain pupil names. High-profile or long-term use of individual pupil images requires specific consent.
- **Website compliance:** The school website will comply with statutory DfE requirements and will credit third-party content appropriately.

12. Parental engagement and support

- **Information and training:** The school will provide parents with clear information about platforms used, safeguarding arrangements for remote lessons and guidance on parental controls. A rolling programme of online safety advice and training will be offered.
- **Communication:** Parents will be informed promptly about incidents affecting their children and given guidance on how to support their child at home.

13. Inclusion and SEND considerations

- **Accessibility:** Remote learning platforms and resources will be assessed for accessibility. The SENCO will coordinate reasonable adjustments and additional support for pupils with SEND.

- **Risk assessment:** Individual risk assessments will be completed for vulnerable pupils to identify and mitigate online risks during remote learning.

14. Monitoring, review and governance evidence

- **Audit trail:** Filtering and monitoring reports, incident logs and training records will be made available to governors and inspectors as part of the school's safeguarding self-evaluation.
- **Review cycle:** This policy will be reviewed at least annually or sooner if there are significant changes to technology, guidance or following a serious incident. The DSL will maintain a record of policy reviews and updates.

15. Training and awareness

- **Staff induction:** Staff receive online safety and data protection training
- **Ongoing CPD:** Annual refresher training and role-specific updates (DSL, ICT, SENCO) are mandatory. Training content is reviewed to reflect emerging threats and guidance.
- **Pupil awareness:** Regular assemblies, lessons and targeted interventions reinforce online safety messages.

16. Useful contacts and external support

- **Designated Safeguarding Lead:** Emma Denty
- **Headteacher:** James Julian
- **Data Protection Officer:** James Julian
- **CEOP (Child Exploitation and Online Protection):** https://www.ceop.police.uk
- **UK Safer Internet Centre:** https://www.saferinternet.org.uk (saferinternet.org.uk in Bing)
- **National Cyber Security Centre (NCSC):** https://www.ncsc.gov.uk

-