



**Nurturing Ambition
Through a Living Faith**

Online Safety Policy

Vision

Our Academy delivers a purposeful curriculum through its living Christian faith. We nurture ambition in all our learners in order for them to become positive citizens of tomorrow.

New Computing Policy.docx

Bible

'Let us not love with words or speech alone but with actions and truth.' — 1 John 3:18

Core Values Online: Perseverance, Courage, Hope, Love, and Friendship apply in the digital world just as they do face-to-face.

Our central ambition is for pupils to become masters of technology, not slaves to it. We view technology as an active educational tool rather than a passive time-filler.

2. Policy Context & Key Legislation

This policy applies to all staff, governors, pupils, and parents/carers. It complies with all current UK legislation and DfE statutory guidance, including:

- **Keeping Children Safe in Education (KCSIE)** (Online safety as a core safeguarding duty)
- **DfE Filtering and Monitoring Standards for Schools**
- **DfE Guidance on Mobile Phones in Schools** (Mobile phone-free environment)
- **DfE Early Years Screen Time Guidance**
- **Education for a Connected World Framework** (UK Council for Internet Safety)
- **Data Protection Act 2018 / UK GDPR & Computer Misuse Act 1990**

3. Leadership, Roles & Responsibilities

- **Designated Safeguarding Lead (DSL) / Online Safety Lead:** Holds overall responsibility for online safety and filtering/monitoring oversight. Maintains up-to-date knowledge and handles disclosure logs.
- **Computing Lead** Supports the DSL, ensures progressive online safety mapping across Purple Mash/PSHE, and audits provision.
- **Cidari IT Support / Network Team:** Maintains real-time dynamic filtering, anti-virus, dynamic AI content blocking, network monitoring, and system logs.
- **All Staff:** Actively supervise digital activity, model safe practice, complete annual online safety training, enforce non-negotiable computing guidelines, and report concerns immediately on MyConcern.

4. Screen Time & Digital Wellbeing

In response to rising screen time outside of school, technology in our classrooms is strictly managed:

- **EYFS & Year 1:** Formal, timetabled computing is delayed until Year 2. Screen exposure in EYFS/Year 1 is strictly limited, completely avoiding solo screen use or passive consumption. Learning focuses on physical technologies (Talking Tins, Beebots, cameras), motor skills, and guided device access (Chromebooks, Mini Mash).
- **Key Stage 1 & 2:** Technology is used as an active learning tool via 1:1 Chromebook provision during planned computing or cross-curricular sessions. Passive screen use, time-filling, or unguided internet browsing is strictly prohibited.
- **Mobile Phones:** The academy operates as a mobile phone-free environment by default for pupils to protect focus, mental health, and physical wellbeing.

5. Generative Artificial Intelligence (AI) Policy

As generative AI tools rapidly evolve, Darwen St James ensures that AI is used ethically, safely, and transparently:

- **Pupil Safety & Data Privacy:** Primary pupils are not permitted to create independent accounts or input personal data (names, addresses, photos) into public AI platforms or LLMs.
- **AI Content Filtering:** School filtering systems actively screen and block unvetted, dynamic AI-generated material that is illegal, age-inappropriate, or harmful.
- **Critical Evaluation:** As part of digital literacy, Key Stage 2 pupils are taught to critically evaluate digital content—recognising that AI tools, deepfakes, and automated search results can produce inaccurate or biased information.
- **Staff Professional Conduct:** Staff utilising AI for lesson planning or administrative efficiency must adhere to UK GDPR regulations. No confidential, identifiable pupil data or safeguarding information may ever be entered into external AI platforms.

6. Online Safety Curriculum & Delivery

Online safety is integrated continuously throughout the academic year rather than treated as an isolated topic:

- **Platform: Purple Mash** is used exclusively for computing curriculum planning and 2Dos.
- **Curriculum Links:** Delivered across Purple Mash computing units, explicit PSHE links, collective worship, and national initiatives (e.g., Safer Internet Day)

- **Four Key Risk Areas (KCSIE):**

1. **Content:** Assessing suitability, validity, radicalisation/extremism risks, copyright, and AI content.
- **Contact:** Managing communication safely, private messaging risks, and reporting unwanted contact.
 - **Conduct:** Preventing cyberbullying, promoting digital kindness (Christian values), protecting passwords, and understanding digital footprints[cite: 1, 3, 4].
 - **Commerce:** Awareness of pop-ups, online scams, phishing, and in-game purchasing hazards.

7. Infrastructure, Filtering & Monitoring

- **Filtering & Monitoring:** Managed via Cidari Trust technical services in alignment with DfE standards. Systems block harmful, illegal, extremist, and inappropriate content across all academy-owned Chromebooks and guest networks.
- **Technical Safeguards:** Personal portable media (e.g., USB sticks) are prohibited. External personal email access is restricted; all pupils and staff use official school Google/Purple Mash accounts.
- **Device Care:** Pupils handle and recharge Chromebooks responsibly, demonstrating stewardship and positive citizenship.

8. Non-Negotiables & Operational Rules

Area	Non-Negotiables for Staff & Pupils
Curriculum Platform	Purple Mash used <i>exclusively</i> for computing; recorded on Planboard.
Pupil Logins	Unique Purple Mash & Google logins used individually; passwords kept private.
Marking & Feedback	All 2Dos are formally marked with unit skill judgements before the next lesson.
EYFS & Year 1	No timetabled standalone computing; hands-on, low-screen exposure only.

Staff Mobile Devices	Personal phones/cameras must not be used for photos or contacting families. School-provided devices used exclusively.
Parental Filming	In line with ICO guidelines, parents/carers are not permitted to video or photograph school performances.

9. Adaptive Provision (SEND Inclusion)

To remove digital barriers and safeguard all pupils, lessons and online platforms are adapted dynamically across the 5 core development areas:

- **Cognitive & Memory:** Visual checklists, unplugged sequencing, and step-by-step coding blocks.
- **Physical Access:** Adapted hardware (joysticks, keyguards, touchscreens).
- **Communication:** Widgit symbols, dual-coding visuals, and Purple Mash audio tools.
- **Sensory & Emotional:** Headphone management, defined partner roles, and co-regulation through explicit debugging routines.
- **Higher-Risk Vulnerability:** DSLs give extra consideration to SEND pupils who may be disproportionately targeted online.

10. Reporting Procedures & Incident Management

Stage 1: Identification & Immediate Logging

- Responsible Party: All Teaching & Support Staff, Pupils
- Actions Required:
 - Log all online safety disclosures, cyberbullying concerns, or inappropriate resource access immediately on MyConcern.
 - Report technical filtering breaches or unsuitable URLs to sjd.ithelpdesk@cidari.co.uk.

Stage 2: Assessment & Triage

- Responsible Party: Designated Safeguarding Lead (DSL) / Headteacher
- Actions Required:
 - Review logged incidents within 24 hours.
 - Assess risk level across KCSIE core areas (*Content, Contact, Conduct, Commerce*).
 - Determine whether internal interventions or external statutory escalations are required.

Stage 3A: Internal Interventions

- Responsible Party: DSL, Headteacher, Class Teacher
- Actions Required:
 - Parental Engagement: Direct, sensitive contact with parents/carers to discuss concerns.
 - Targeted Education: Provide additional 1:1 or class online safety input.
- System Restrictions: Temporarily remove or restrict internet and computer access if required.
- Record Keeping: Document all actions and consequences on MyConcern.

Stage 3B: External Escalations

- Responsible Party: DSL, Headteacher, Cidari IT Lead
- Actions Required:
 - Multi-Agency Safeguarding: Refer to Children's Social Care / MASH where statutory thresholds are met.
 - Law Enforcement / CEOP: Contact Police or CEOP in cases of online grooming, severe harassment, or illegal acts.
 - Illegal Content: Report illegal online material directly to the Internet Watch Foundation (IWF).
 - Trust Technical Escalation: Inform the Cidari E-Learning Manager to block domains network-wide.

Reporting:

Unsuitable web content or disclosures must be logged on MyConcern and emailed to sjd.ithelpdesk@cidari.co.uk.

1. **Handling:** Concerns are managed sensitively by the DSL and Senior Leadership. Sanctions follow the Academy Behaviour Policy (counselling, parental meetings, restricted system access).
2. **Escalation:** Illegal material is escalated directly to the Internet Watch Foundation (IWF) or the Police/CEOP.

11. Policy Review & Governance

- **Review Cycle:** Reviewed annually by the Computing Lead, DSL, Headteacher, and Link Governor.
- **Staff Sign-Off:** All staff must read, sign, and adhere to the Acceptable Use Policy (AUP) annually.
- **Auditing:** Half-termly monitoring (drop-ins, work scrutiny, pupil voice) and annual DfE filtering audits ensure full compliance

-

