E-SAFETY

POLICY

CRUMLIN
INTEGRATED
COLLEGE

RATIFIED: 22 MAY 2026
REVIEW DATE: JUNE 2028

Contents

1. Introduction, Ethos, and School Context

At Crumlin Integrated College, our core ethos is centered on equality, inclusion, parental involvement, and social responsibility. We recognise that digital technologies and internet access are integral to facilitating rich learning opportunities; however, we hold an absolute duty of care to ensure our school community remains safe, secure, and supported in digital spaces.

This policy is guided directly by our core school mantra: **"Each Student, Each Journey, Every Success"** and is explicitly framed around our **CRUMLIN** values:

- **Community:** Building an interconnected network of pupils, staff, and parents who collaborate to maintain a safe and supportive digital environment.
- **Respect:** Ensuring that all online communications are polite, professional, and respect the rights and dignity of every individual.
- **Unity:** Working collectively across all stakeholders to implement robust protective and educational measures against online harms.
- **Motivation:** Empowering our pupils to become confident, discerning, and positive digital citizens who make informed online choices.
- **Leadership:** Demonstrating accountability, explicit professional boundaries, and excellent digital modeling at all staff and governor levels.
- **Inclusion:** Providing accessible, equitable digital protections and interventions tailored to meet the diverse needs of all learners.
- **Nurture:** Prioritising early intervention, pastoral support, and safeguarding-led restorative responses when digital incidents occur, rather than focusing solely on punitive actions.

2. Purpose and ETi Inspection Statement

This E-Safety Policy has been developed in strict alignment with the Education and Training Inspectorate (ETi) safeguarding evaluation expectations. It serves to evidence that Crumlin Integrated College:

- Maintains clear governance, strategic leadership, and administrative oversight of online safety.
- Embeds electronic safety within our overarching safeguarding frameworks, pastoral care models, and cross-curricular structures.
- Implements highly effective, proportionate filtering, monitoring, and reporting mechanisms.
- Delivers robust preventative education and early intervention systems alongside an accountable response structure.
- Complies with all current Northern Ireland legislation, Department of Education (DE) Circulars, and statutory guidance.

3. Legislative and Statutory Compliance

This policy complies fully with and reflects the requirements of the following statutory frameworks:

- **Education and Libraries (Northern Ireland) Order 2003** (Articles 17 & 18 — Safeguarding duties of Boards of Governors).
- **DE Circular 2016/27** — Online Safety (Mandatory Guiding Principles).
- **DE Circular 2017/04 (Updated 2023)** — Safeguarding and Child Protection in Schools.
- **Addressing Bullying in Schools Act (NI) 2016** (including statutory mandates on tracking and responding to cyberbullying).
- **UK GDPR & Data Protection Act 2018**.
- **The Online Safety Act 2023**.
- **Online Safety Strategy for Northern Ireland 2022–2027**.

4. Integration with the School Safeguarding Framework

Online safety at Crumlin Integrated College is explicitly managed as a **safeguarding and pastoral issue, not an ICT technical issue**. This document works in direct conjunction with the following school policies:

- **Safeguarding & Child Protection Policy:** Governs serious harm, exploitation, child-on-child abuse, grooming, or cases requiring immediate external referral.
- **Positive Behaviour Policy:** Outlines the clear ladder of interventions, restorative practices, and proportionate behavioral sanctions applied when school rules regarding technology or mobile devices are broken.
- **Pastoral Care Policy:** Guides the tailored support, emotional well-being, and therapeutic follow-up provided to students who have been victims of online harms or digital isolation.
- **Educational Visits Policy:** Extends e-safety protocols to off-site learning. While participating in school field trips, residentials, or sports excursions, pupils must adhere to the same Acceptable Use standards. Staff must maintain rigorous professional boundaries during digital updates and are mandated to ensure that any capturing or sharing of trip media follows strict school-device protocols.

5. Scope and Definition of Online Safety Risks

This policy applies to all members of the college community—including governors, staff, pupils, volunteers, parents/carers, and visitors—who access school ICT infrastructure, use school devices, or bring personal mobile devices onto school grounds. It also covers online actions occurring out of school if they are connected to membership of the college community.

In line with Department of Education guidance, online safety risks are categorised across the following dimensions:

- **Content:** Exposure to illegal, inappropriate, harmful, violent, or extremist material.

- **Contact:** Grooming, exploitation, peer coercion, or harmful, unsolicited interaction with strangers.
- **Conduct:** Cyberbullying, targeted digital harassment, image-based abuse, and harmful sexual behavior.
- **Commerce:** Commercial scams, phishing, online gambling, personal data harvesting, or financial exploitation.
- **Technology-enabled Safeguarding Risks:** Digital behaviors indicating self-harm, suicide ideation, online radicalisation, or severe exposure to misinformation.

6. Roles and Responsibilities

6.1 The Board of Governors

- Provides strategic governance and final approval for this policy, reviewing its efficacy annually.
- Appoints a designated **Safeguarding Governor** who is kept informed of incident patterns, monitors anonymised logs, and audit filtering and change-control system adjustments.
- Ensures that appropriate budget, resource allocations, and statutory staff training remain compliant with Education Authority (EA) standards.

6.2 The Principal and Senior Leadership Team (SLT)

- Maintains ultimate operational duty of care for ensuring online safety across the college.
- Ensures that EA/C2k filtering and monitoring systems are configured correctly and that automated risk alerts are actively addressed.
- Ensures that a designated lead is appointed and that all staff undergo regular statutory child protection and online safety professional development.
- Implements clear operational pathways to handle serious online safety allegations made against any member of staff.

6.3 Designated Child Protection Officer (DCPO) / Designated Teacher

- Acts as the primary school lead for managing online safeguarding referrals and checking them against statutory thresholds.
- Maintains secure, confidential safeguarding records of all electronic incidents.
- Coordinates directly with external agencies—such as EA Support Services, Social Services, or the Police Service of Northern Ireland (PSNI)—whenever an incident crosses a legal or child protection threshold.

6.4 E-Safety Coordinator / E-Learning Lead

- Manages day-to-day online safety issues and updates internal guidance charters.
- Maintains the operational E-Safety Incident Log to analyse internal trends and adjust the preventative curriculum accordingly.

- Liaises with C2k management, technical personnel, and the E-Safety Governor to optimise school network security.

6.5 C2k Manager and Technical Support Personnel

- Ensures the college infrastructure is secure, password protocols are strictly enforced, and network changes are logged.
- Monitors network usage and logs proxy-avoidance attempts, immediately flagging any network misuses to the SLT or E-Safety Coordinator.

6.6 Teaching and Support Staff

- Treat online safety strictly as an active safeguarding responsibility.
- Read, understand, sign, and adhere to the E-Safety Policy.
- Maintain strict professional digital boundaries. All digital communications with students or parents must be conducted using official school channels (e.g., C2k, official VLE); staff must never share personal mobile numbers or connect via personal social media accounts.
- Actively monitor classroom technology use. In pre-planned lessons using YouTube or the internet, staff must fully preview video clips and sites beforehand; searches should never be conducted live in full view of the class to avoid generating inappropriate ad-hoc results.

6.7 Pupils

- Are expected to protect their personal login usernames and passwords, never sharing them or using another pupil's account.
- Must immediately report any inappropriate content, distressing messages, or cyberbullying directed at themselves or others to a trusted member of staff.
- Must ensure all devices on their person are switched off whilst they are on school premises

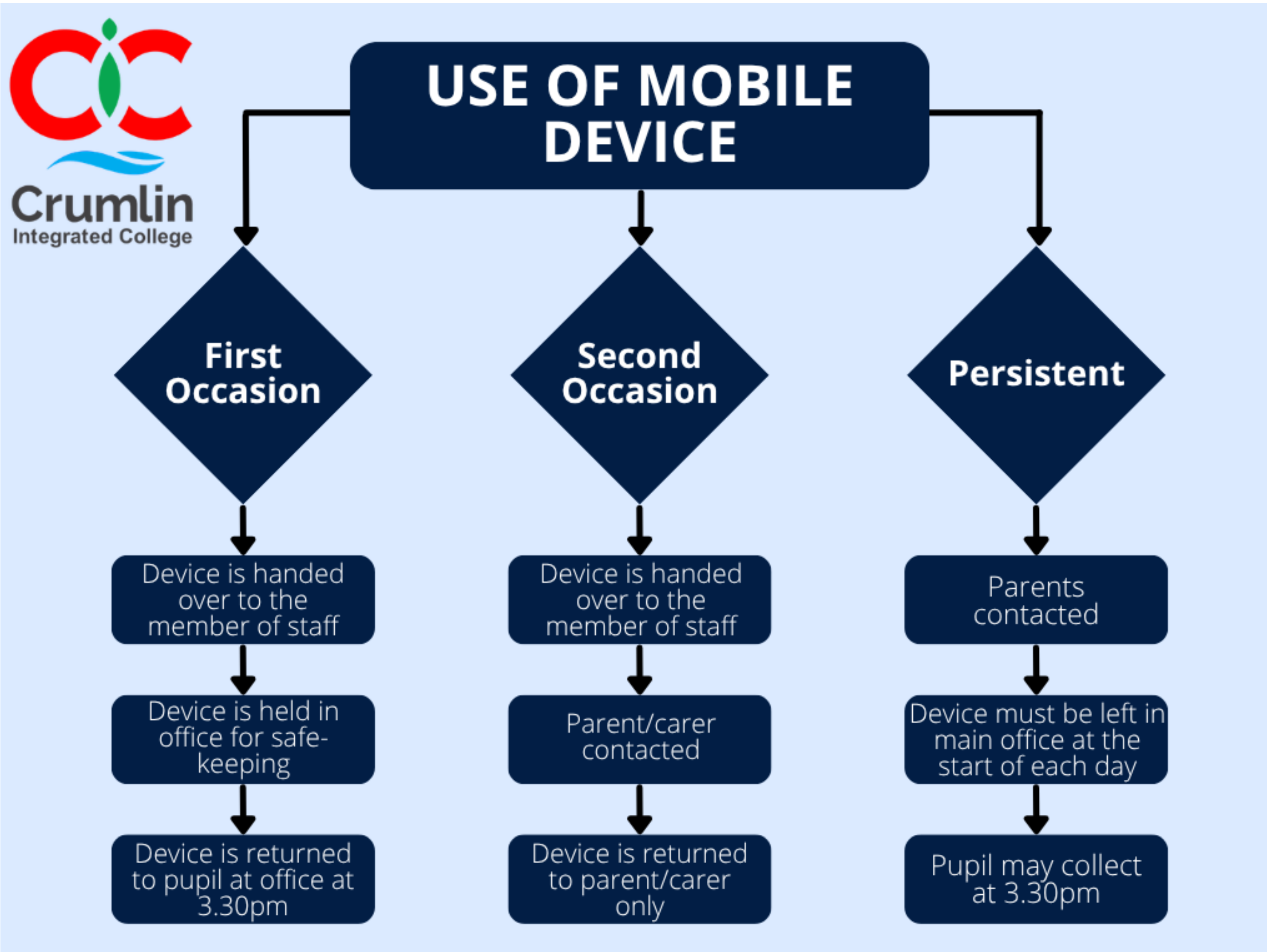
6.8 Parents and Carers

- Are expected to act as partners with the college by reinforcing responsible internet and device boundaries at home.
- Are encouraged to regularly engage with school information evenings, safety campaigns, and guidance materials provided via school platforms.

7. Acceptable Use of Technology and Mobile Devices

- Mobile Phone Infrastructure: Student mobile device usage must adhere strictly to current DE directives and school positive behavior matrices. Devices are to remain off and stored away unless explicit permission is granted by a teacher for targeted, distinct educational applications.

- **Device Misuse Framework:** In line with our nurturing ethos, initial or low-level technology misuse is handled via early intervention, pastoral guidance, and positive behavioral strategies, rather than an exclusively punitive response.
- The following steps are taken to prevent and limit the misuse of devices during the school day:



8. Filtering, Monitoring, and Data Protection

- Crumlin Integrated College implements the mandatory **EA-approved C2k filtering and monitoring network**. Automated content filters are systematically updated to block illegal, extremist, or harmful websites.
- Network logs are monitored regularly for performance, proportionality, and systemic alerts.
- All data storage, pupil data tracking, and remote system accesses adhere to rigorous UK GDPR and Data Protection Act 2018 standards. High-risk monitoring alerts (e.g., self-harm searches) trigger an immediate safeguarding escalation path to the DCPO.

9. Preventative Online Safety Education

Recognizing that mechanical filtering must be reinforced with user resilience, the college embeds a structured, progressive digital safety curriculum across all key stages:

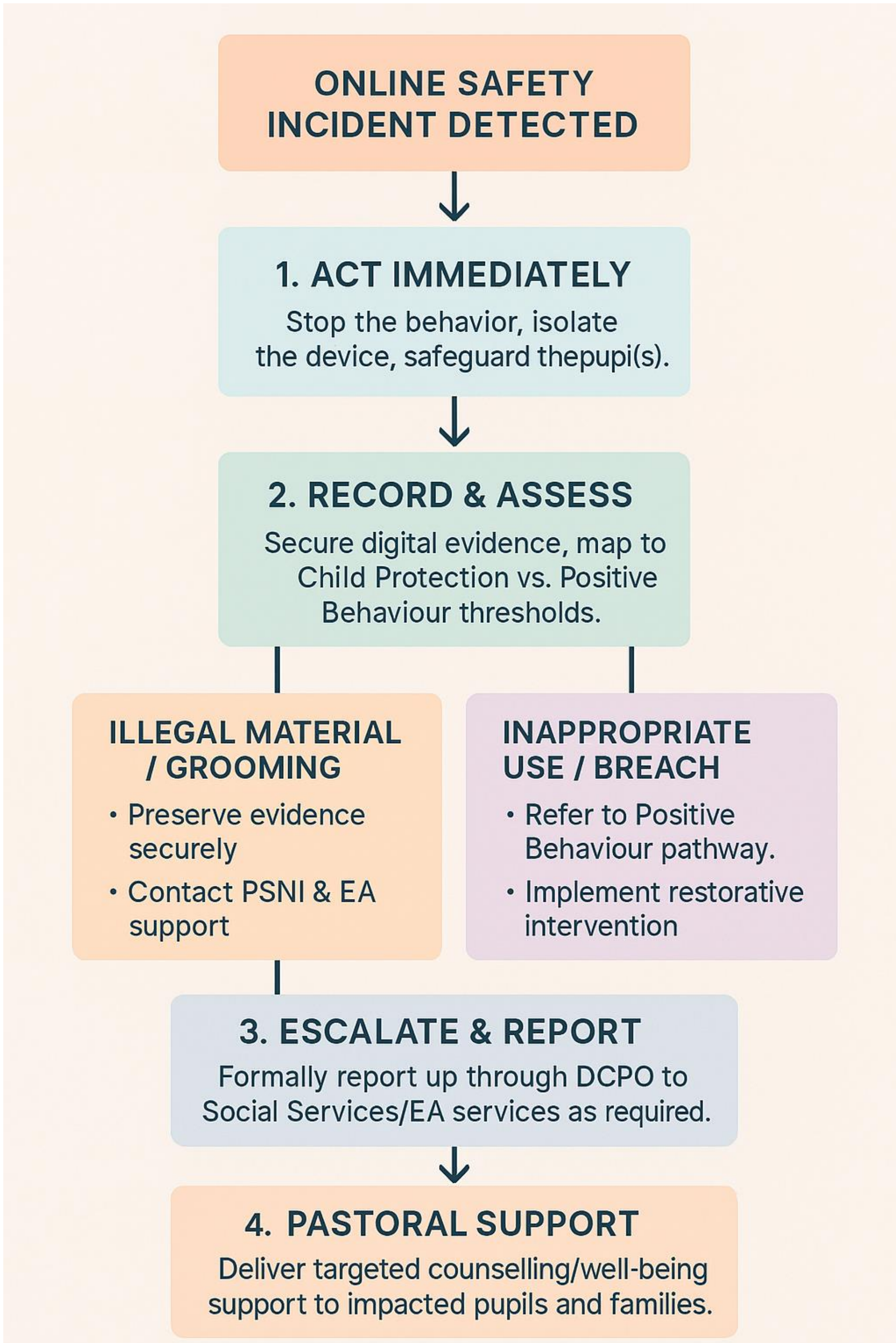
- **Curriculum Delivery:** Age-appropriate modules covering content verification, copyright respect, privacy settings, and the dangers of grooming are explicitly taught within ICT, Learning for Life and Work (LLW), and Relationship and Sexuality Education (RSE).
- **Whole-School Integration:** E-safety messages are regularly consolidated through pastoral tutor periods, school assemblies, and high-profile collaborative frameworks like *Safer Internet Day*.

10. Digital Images, Video, and Social Media Controls

- **Official School Accounts:** The college operates designated social media channels (e.g., official Facebook/Instagram profiles) solely to showcase school activities and celebrate student success. These are strictly managed by an authorised coordinator and overseen by the SLT.
- **Image Protections:** Written parental consent must be obtained before any pupil image or video is published online. Full names of pupils will never be published alongside or appended to photographs.
- **Equipment Mandate:** Staff are strictly prohibited from using personal mobile devices or personal cameras to record pupils or take media during school hours or educational visits; only school-issued hardware may be used.
- **Public Events Policy:** Parents and carers are welcome to capture images or video at open school assemblies or sports events for personal use. However, to protect vulnerable children, these images must not be uploaded to public social media if they contain identifiable pictures of other pupils.

11. Incident Response and Cyberbullying Procedures

The college applies an immediate, 5-step operational architecture whenever an online safety incident or infraction is identified:



- **Cyberbullying:** Cyberbullying is treated strictly as a major safeguarding issue, not a minor behavioral issue. It will be countered in full compliance with the *Addressing Bullying in Schools Act (NI) 2016*. The college prioritises tracking patterns, emotional impact, and the underlying vulnerability of the targeted pupil over treating incidents as isolated occurrences.

12. Policy Monitoring, Review, and Quality Assurance

To remain responsive to evolving technological trends and statutory changes, this policy undergoes systematic annual quality assurance.

13. Declaration

This policy represents an active, transparent commitment to ensuring effective, proportionate, and accountable digital safety practice that meets ETi inspection standards and ensures the safe journey of every student.