Chevin Academy Online Safety Policy (2025)

1. Introduction

Chevin Academy acknowledges the critical importance of safeguarding children and young people in all aspects of their online lives. This Online Safety Policy is an integral part of the academy's overarching safeguarding framework and supports statutory obligations under the Children Act 1989/2004, the Data Protection Act 2018, the GDPR, the Online Safety Act 2023, and the Department for Education's Keeping Children Safe in Education (KCSIE) 2025 statutory guidance. It is designed to protect all users from the risks associated with digital technologies while promoting a culture of responsible digital citizenship.

2. Purpose

The purpose of this policy is to:

- Protect learners, staff, and stakeholders from all forms of online harm including cyberbullying, exploitation, exposure to illegal or inappropriate content, misinformation, and risks linked to emerging technologies such as AI.
- Ensure compliance with statutory duties for safeguarding and data protection.
- Define clear roles and responsibilities for online safety management across the academy.
- Embed online safety education into the academy ethos, curriculum, and pastoral care.

3. Scope

This policy applies to:

- All learners including those in alternative provision and SEND.
- All staff, volunteers, contractors, and governors.

- All digital technologies used on-site, remotely, and personally where they interface with academy functions, resources, or learners.

4. Statutory Framework & Guidance

This policy incorporates requirements from:

- Keeping Children Safe in Education (KCSIE) 2025: Including new expectations for filtering, monitoring, and responding to harmful content and behaviour.
- Online Safety Act 2023: Imposing a duty of care on platforms, requiring risk assessments and mitigation of online harms.
- Children Act 1989 & 2004: Safeguarding and promoting welfare of children.
- Data Protection Act 2018 & GDPR: Governing personal data handling and privacy.
- UK Safer Internet Centre Best Practices and Guidance.

5. Roles and Responsibilities

Senior Leadership Team (SLT):

- Ultimate accountability for online safety and safeguarding compliance.
- Ensure robust filtering and monitoring systems are in place, tested regularly as required by KCSIE 2025.
- Manage the handling and escalation of online safety incidents.
- Allocate sufficient resources for training, technology, and policy implementation.

Designated Safeguarding Lead (DSL) and Deputies:

- Lead and coordinate online safety strategy and response.
- Act as the first point of contact for online safety incidents and concerns.
- Liaise with external safeguarding agencies, the local authority, and law enforcement.
- Maintain detailed records of online safety incidents and actions taken.

- Support staff and learners in understanding and managing risks, including those related to emerging technologies.

IT and Network Managers

- Implement, maintain, and review effective filtering and monitoring technologies aligned with statutory requirements.
- Conduct regular system audits, testing, and reporting to SLT and DSL.

Staff

- Promote responsible use of technology in teaching and support roles.
- Supervise learner use of devices and platforms, applying the Acceptable Use Policy consistently.
- Participate in regular online safety training.
- Promptly report any online safety concerns or incidents following academy procedures.

Students

- Adhere to the Acceptable Use Agreement (AUA) detailing expectations for safe, respectful, and responsible use of technology which will be part of student induction and continuously and regularly communicated
- Report any online safety concerns, including bullying, grooming, or exposure to harmful content, to staff immediately.
- Engage with online safety education tailored to their developmental needs and abilities.

Parents and Carers

- Support academy policies and guidance on learner technology use at home.
- Engage with online safety communications and training.
- Report any concerns or observed risks about their child's online safety.

6. Online Safety Procedures

Online Safety Education and Curriculum Integration

- Embed online safety into PSHE, safeguarding education, and curriculum subjects using age-appropriate materials including UK Safer Internet Centre resources.
- Provide specific training tailored to learners with SEND or additional vulnerabilities.
- Raise awareness of new risks including those posed by generative AI, misinformation, and online radicalisation.
- Encourage learner critical thinking and digital literacy skills.

Acceptable Use Agreements (AUA)

- All staff, learners, parents, and visitors must sign an AUA specifying expected behaviours and consequences of breaches.
- Review AUAs annually or upon any changes in technology or policy.

Filtering and Monitoring

- Deploy advanced filtering technology to block access to illegal and inappropriate content, including new categories such as misinformation and conspiracy theories per KCSIE 2025.
- Students will not have access to the Wifi connection unless through a Chevin Academy device which will have been set up for their use (they will not have password access).
- IT security systems are in place such as using a cloud based Demain Name System, Windows Defender firewall and the use of Microsoft Education
- Safe, responsible and ethical use of mobile phone and social media will be covered through Student Induction and the sharing of personal mobile and social media details will be discouraged (as a post-16 provider unless there is a Mental Capacity Act assessment that states otherwise Chevin Academy cannot stop students sharing these

should they wish to do so outside of the education provider). Any violation of this would be covered under the behaviour policy.

- Mobile phones and personal IT should be switched off during learning times, unless specific strategies / applications are required for learning.
- Implement real-time or near real-time monitoring to detect safeguarding risks promptly.
- Test and review filtering and monitoring systems at least termly, documenting effectiveness and any incidents.

Cyberbullying and Online Harassment

- Zero tolerance policy, aligned with the Behaviour and Anti-bullying Policy.
- Provide confidential reporting channels and support mechanisms for victims.
- Investigate incidents thoroughly, with involvement of DSL and safeguarding partners as needed.
- Positive online behaviour campaigns and restorative approaches.

Data Protection and Privacy

- Comply fully with GDPR and Data Protection Act 2018 in all online safety practices.
- Protect learner and staff data with secure credentials, encryption where applicable, and strict access controls.
- Provide guidance on safe password practices and account management.
- Conduct regular audits and staff training on data protection responsibilities.

Incident Management and Reporting

- Maintain a detailed online safety incident log with anonymised data respecting confidentiality.
- Follow the academy safeguarding referral pathway for serious or criminal concerns including notification to local authority and/or police.
- Report and cooperate with Phishing, hacking, or other cybercrime incidents with appropriate external agencies.
- Review incidents to identify trends, update policies, and enhance training.

Use of Technology and Platforms

- Personal Devices will not be permitted for use during learning time unless specific strategies / applications are required for learning. If this is required this will be detailed as part of the student support plan, under staff oversight.

Social Media and Communication

- Only approved platforms may be used to communicate with learners and parents.
- Staff must maintain professional boundaries and use academy email or communication tools.
- Learners educated on risks related to social media, including privacy settings and digital footprint.

Remote Learning and Virtual Schooling

- Only secure platforms with controlled access and supervision to be used.
- Reinforce online safety norms, privacy, and reporting mechanisms during remote sessions.

7. Compliance and Governance

The Online Safety Policy will be reviewed annually or when legislation changes.

Director will commission independent audits of technology, policy, and training effectiveness.

Provide regular updates to staff, governors, learners, and parents.

Maintain records of training, incidents, reviews, and actions taken.

8. Related Policies

Safeguarding and Child Protection Policy

Behaviour Policy

Data Protection and GDPR Policy

Staff Code of Conduct

Anti-Bullying Policy

Use of Mobile Devices Policy

Remote Learning Policy

9. Approval and Review

This policy is authorised by Chevin Academy CIC Directors and Senior Leadership Team. It is reviewed annually and following any major online safety incidents or legislative changes.