Cornwall Education Learning Trust

Online Safety Policy

Safeguarding Policy Suite

Cornwall Education Learning Trust Policies
Cornwall Education Learning Trust (CELT), Atlantic Centre, Trenance Leisure Park, Newquay, Cornwall TR7 2LZ

Our Mission

At Cornwall Education Learning Trust (CELT), our mission is clear: to provide every learner with an **exceptional educational experience.** One that enables them to thrive, achieve and succeed in life. We believe in a **100%** mindset, that every learner, in every classroom, in every school, deserves the very best we can offer. For us, 100% means no compromise: no learner left behind, no community overlooked, and no opportunity wasted.

Our strategic goals reflect this ambition. We are committed to empowering and growing our people, building an ambitious all-through entitlement, forging exceptional relationships with our communities, transforming provision through meaningful partnerships, and leading an ethical, effective and innovative organisation. These are not just aspirations; they are promises that shape the way we work and the culture we are building together.



Our Values

Our values are at the heart of everything we do. We believe in the power of **Collaboration**, building strong relationships and working together as one team to achieve our collective goals. We are committed to **Empowerment**, creating a culture where initiative, innovation and trust flourish, and where every individual feels valued, respected and motivated.

As a Trust, we are grounded in promoting **Leadership**, sharing a moral and ethical purpose to improve the lives of others and make a lasting difference for our learners and communities. And we embrace **Transformation**, approaching change positively so that we can all become our best selves and do our best work.

These values guide every decision we make and every action we take. They are the foundation of our Trust and the reason we can offer such exceptional opportunities for our learners and staff. If you choose to join CELT, you will be part of a values-driven organisation where people are supported to grow, contribute, and thrive.

Policy Contents

1. Policy Overview 4
   1.1 Policy Purpose and Aims **Error! Bookmark not defined.**
   1.2 Policy Approval and Review 4
   1.3 Policy Version History 4
2. Policy Introduction and Framework 5
   2.1 Introduction 5
   2.2 Legislation and Statutory Framework 5
3. Purpose and Scope 6
4. Understanding online risk 6
5. Roles and responsibilities 7
   5.1 Trustees 7
   5.2 Headteachers 7
   5.3 Designated Safeguarding Lead 7
   5.4 Trust digital and IT leads 7
   5.5 All staff 8
   5.6 Parents/Carers 8
   5.7 Learners 8
6. Safeguarding and online harm 8
7. Teaching online safety 9
8. Filtering and monitoring 9
9. Acceptable use 10
10. Cyber security and data protection 10
11. Reporting and responding to online safety incidents 10
12. Staff training 11
13. Monitoring, assurance and review 11

Appendix 1 – Learner Acceptable Use Agreement: EYFS/KS1 12
Appendix 2 – Learner Acceptable Use Agreement: KS2 13
Appendix 3 – Learner Acceptable Use Agreement: KS3–KS5 14
Appendix 4 – Staff Acceptable Use Agreement 15
Appendix 5 – Visitor, Volunteer and Contractor Acceptable Use 16

1. Policy Overview

1.1 Safeguarding commitment

"It could happen here." We recognise our moral and statutory responsibility to safeguard and promote the welfare of all children. We make every effort to provide an environment in which children and adults feel safe, secure, valued and respected, and feel confident to talk if they are worried, believing they will be effectively listened to. The purpose of this policy is to provide staff, volunteers and governors with the framework they need in order to keep children safe and secure at Cornwall Education Learning Trust (CELT). The policy also informs parents and carers how we will safeguard their children whilst they are in our care.
children whilst they are in our care.

At Cornwall Education Learning Trust (CELT) we are committed to safeguarding and promoting the welfare of children and we expect all trustees, community champions, staff and volunteers to share this commitment. This policy is part of the following suite of annually updated safeguarding policies.

1.2 Policy Approval and Review

Policy Version Number:	4
Approved By:	Trustees
Approved On (Date):	
Review Period:	Annually

This policy will be reviewed at least annually and updated sooner where legislation, statutory guidance, technology or identified safeguarding risks require it.

Filtering and monitoring arrangements will be formally reviewed at least annually and whenever significant changes or concerns require an earlier review.

This policy is available publicly through the school website.

1.3 Policy Version History

Policy Version	Date Issued	Summary of Changes
1	30.11.22	First Issue – No Changes
2	24.08.24	Annual review
3	18.08.2026	Update of content harm, additional indicators of Concerns about learners welfare
4	09.08.2026	Updated in line with KCSIE 26 Filtering and monitoring Understanding online risk Acceptable use appendices

2. Policy Introduction and Framework

2.1 Introduction

Cornwall Education Learning Trust (CELT) recognises that technology is an integral part of education and of learners' lives. Used safely and responsibly, digital technology provides significant opportunities for learning, communication, creativity and participation. It can also expose children and adults to harm.

Online safety is therefore an integral part of safeguarding and is not treated as a separate or solely technical issue. CELT takes a whole-Trust approach which combines effective safeguarding practice, education, appropriate filtering and monitoring, secure technology, clear expectations for acceptable use and effective responses when concerns arise.

Our approach is underpinned by the principle that safeguarding children online is as important as safeguarding them offline. We will seek to ensure that every learner is seen, heard, known and valued and is equipped with the knowledge, skills and confidence to use technology safely, responsibly and respectfully.

This policy should be read alongside CELT's Safeguarding and Child Protection Policy, Child-on-Child Abuse and Anti-Bullying Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, Artificial intelligence policy and other relevant safeguarding and information-security procedures.

2.2 Legislation and Statutory Framework

This policy has regard, where applicable, to:

- Children Acts 1989 and 2004;
- Education Act 2002;
- Education and Inspections Act 2006;
- Equality Act 2010, including the Public Sector Equality Duty;
- Data Protection Act 2018 and UK GDPR;
- Online Safety Act 2023;
- Keeping Children Safe in Education 2026;
- Working Together to Safeguard Children 2026;
- Prevent Duty Guidance;
- Counter Terrorism and Security Act 2015
- statutory Relationships Education, Relationships and Sex Education and Health Education guidance applicable from September 2026;
- DfE Filtering and Monitoring Standards for Schools and Colleges;
- DfE Cyber Security Standards for Schools and Colleges;

- DfE Teaching Online Safety in Schools guidance;
- DfE Generative Artificial Intelligence in Education guidance and associated product safety standards;
- DFE Technical Standards
- UKCIS guidance on Sharing Nudes and Semi-Nudes;
- DfE Searching, Screening and Confiscation guidance;
- statutory Mobile Phones in Schools guidance; and
- the statutory framework for the Early Years Foundation Stage, where applicable.

CELT will keep its arrangements under review as technology, legislation and national guidance develop.

3. Purpose and Scope

This policy sets out CELT's strategic approach to:

- protecting learners from online harm;
- providing effective online safety education;
- establishing expectations for safe, lawful and responsible use of technology;
- ensuring appropriate filtering and monitoring arrangements;
- identifying and responding to online safeguarding concerns;
- supporting learners who may be particularly vulnerable online;
- managing emerging technologies, including generative artificial intelligence (AI);
- promoting appropriate professional use of technology by staff; and
- working with parents, carers and relevant agencies to keep learners safe.

It applies to all CELT schools and to learners, employees, agency staff, volunteers, contractors, trustees, community champions and other people who access CELT technology, networks or digital services.

It applies to Trust-owned and personal devices where these are used on CELT premises, connected to CELT networks or systems, or used in connection with CELT business.

4. Understanding online risk

CELT recognises the four broad areas of online risk identified within Keeping Children Safe in Education:

Content – being exposed to illegal, inappropriate or harmful content for example: pornography, racism, misogyny, antisemitism, self-harm, suicide, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

Contact – being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,

Conduct – online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying.

Commerce – risks including inappropriate advertising, scams, phishing, financial exploitation, gambling and other commercial practices which may cause harm.

These risks can overlap and may form part of wider safeguarding concerns including child sexual exploitation, child criminal exploitation, radicalisation, child-on-child abuse, domestic abuse, sexual violence and harassment, coercive control and mental health concerns.

CELT recognises that technology changes rapidly. Online safety arrangements will therefore consider emerging and evolving risks rather than relying solely upon lists of particular applications, websites or technologies.

5. Roles and responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

5.1 Trustees

The Trust Board will ensure that CELT has appropriate arrangements to safeguard learners online, including effective filtering and monitoring, appropriate policies, staff training and oversight.

Trustees will receive appropriate assurance regarding the effectiveness of these arrangements.

5.2 Headteachers

Headteachers are responsible for ensuring that this policy is implemented within their school and that online safety is embedded within safeguarding, curriculum, behaviour and operational arrangements including all staff receive appropriate online safety training and their responsibilities in relation to filtering and monitoring.

5.3 Designated Safeguarding Lead

The DSL has lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place.

The DSL will ensure that online safeguarding concerns are identified, assessed, recorded, responded to and escalated appropriately.

5.4 Trust digital and IT leads

Those responsible for technology will work with safeguarding leaders to maintain secure systems and effective filtering and monitoring arrangements, identify technical risks and ensure appropriate action is taken when concerns or deficiencies arise.

Technical staff do not determine safeguarding outcomes independently of the DSL.

5.5 All staff

All staff must:

- understand that online safety is part of safeguarding;
- understand the school's filtering and monitoring arrangements;
- remain vigilant to online harm;
- model safe and professional technology use;
- follow the relevant Acceptable Use Agreement; and
- report safeguarding concerns to the DSL or deputy without delay.

5.6 Parents/Carers

Parents and carers are encouraged to discuss technology use with their children, engage with the relevant information shared with families, establish appropriate boundaries and report concerns to school where online activity may affect their child's welfare.

5.7 Learners

Learners will be supported to use technology safely, respectfully and responsibly, report concerns and seek help when something online worries, frightens or harms them.

6. Safeguarding and online harm

Online safety is an integral part of safeguarding. Any concern that a learner may be experiencing, or be at risk of, harm online must be reported to the Designated Safeguarding Lead (DSL) or deputy without delay and managed in accordance with CELT's Safeguarding and Child Protection Policy.

Online behaviour outside school may also fall within CELT's safeguarding or behaviour responsibilities where it affects the welfare of a learner, members of the school community or the safe and orderly operation of the school. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

The DSL will assess and respond to online safeguarding concerns in accordance with statutory safeguarding guidance and CELT procedures, including making referrals to children's social care, the police or other agencies where appropriate, involving parents and carers where it is safe and appropriate to do so, ensuring appropriate support for learners, and recording decisions and actions.

Where online behaviour constitutes or forms part of child-on-child abuse, including sexual violence, sexual harassment, bullying, harmful sexual behaviour or abuse within intimate personal relationships, CELT's Child-on-Child Abuse including Anti-Bullying Policy and behaviour policy will also apply.

CELT will work with safeguarding partners and relevant agencies where coordinated help, support or protection is required.

7. Teaching online safety

CELT will provide age-appropriate, developmentally appropriate and inclusive online safety education that equips learners with the knowledge, understanding and skills to recognise risk, make informed decisions, behave responsibly and seek help when needed.

Online safety will be embedded as a running and interrelated theme across the curriculum, including through Relationships Education, Relationships and Sex Education (RSE), Health Education, Computing and wider safeguarding education. Teaching will reflect statutory curriculum requirements, current and emerging online risks and the needs and experiences of learners.

Education will support learners to understand how to build safe and respectful relationships; protect their privacy, wellbeing and personal information; recognise harmful, abusive, exploitative, discriminatory or misleading content and behaviour; use technology, social media and emerging technologies, including generative AI, safely and responsibly; and understand how to report concerns and access support.

Teaching will be inclusive and sensitive to learners' individual circumstances and vulnerabilities. Where a learner is known to have experienced abuse or harm, reasonable care will be taken to ensure that curriculum delivery does not inadvertently identify, distress or further harm them.

8. Filtering and monitoring

CELT recognises filtering and monitoring as an integral part of its safeguarding arrangements and will maintain appropriate systems to limit learners' exposure to harmful and inappropriate online content and activity. Smoothwall is used across the Trust to provide filtering and monitoring of school networks and school-managed devices.

Filtering and monitoring arrangements will be proportionate to the age, needs and risk profile of learners and will support, rather than replace, effective supervision, online safety education and professional safeguarding practice.

Clear responsibilities will be established for the oversight and management of filtering and monitoring. Relevant staff will understand the arrangements in place, their responsibilities and how to escalate safeguarding concerns or identified weaknesses without delay.

The effectiveness of filtering and monitoring will be formally reviewed at least once each academic year and following significant changes or identified risks. Reviews will include appropriate checks across internet-connected devices and relevant locations, consider emerging technologies and risks including generative AI, and be recorded.

Trustees will maintain strategic oversight and receive appropriate assurance that filtering and monitoring arrangements are effective and meet CELT's safeguarding responsibilities.

9. Acceptable use

All users of CELT technology and networks are expected to use them safely, responsibly, lawfully and respectfully.

Appropriate Acceptable Use Agreements will apply to:

- learners, differentiated according to age and developmental understanding;
- employees;
- volunteers and contractors; and
- visitors or other authorised users where appropriate.

Users will be made aware that activity on CELT systems and networks are filtered, logged and monitored for safeguarding, security and compliance purposes in accordance with applicable law and CELT privacy information.

Access to CELT technology is conditional upon compliance with this policy and the relevant Acceptable Use Agreement. Detailed Acceptable Use Agreements are contained in the appendices to this policy.

10. Cyber security and data protection

CELT recognises effective cyber security and data protection as leadership and governance responsibilities and as integral to maintaining a safe and resilient digital environment. The Trust will maintain proportionate arrangements to prevent, detect, respond to and recover from cyber-security incidents, supported by appropriate oversight, staff awareness, business continuity and incident-response arrangements.

All users are expected to use CELT systems, devices, information and digital services securely and responsibly and to report suspected security incidents, data breaches or vulnerabilities promptly.

Detailed requirements are set out in CELT's data protection, information security, cyber-security and acceptable-use policies and procedures.

11. Reporting and responding to online safety incidents

All online safety incidents and concerns must be reported promptly through the school's agreed reporting and recording arrangements. Learners, parents and carers will be provided with clear and accessible ways to report online safety concerns, including where they are worried about themselves or another learner.

Staff must report any online safety concern involving actual or suspected harm, abuse, exploitation or risk to a learner to the Designated Safeguarding Lead (DSL) or deputy without delay. Where there is a safeguarding concern, CELT's Safeguarding and Child Protection Policy and safeguarding procedures take precedence.

Online safety incidents will be considered according to their nature, context and level of risk and will not be treated solely as behaviour, disciplinary or IT matters. Responses will be proportionate, child-centred and informed by the impact, intent, age, vulnerability and needs of those involved.

Depending on the nature of the incident, CELT's other policies and procedures may also apply, including the Child-on-Child Abuse and Anti-Bullying Policy, Behaviour Policy, Managing Allegations Policy, Staff Code of Conduct, disciplinary procedures, Data Protection Policy and cyber-security or information-security procedures.

Where an incident may constitute a criminal offence or require statutory intervention, the DSL or appropriate senior leader will consider referral to the police, children's social care or other relevant agencies in accordance with safeguarding procedures.

Staff must preserve relevant evidence appropriately and must not undertake their own investigation where this could increase risk to a learner or compromise a safeguarding or police investigation. All actions, decisions and outcomes will be recorded through the appropriate school systems.

12. Staff training

All staff will receive appropriate online safety training as part of induction and safeguarding training, with regular updates to reflect emerging risks, technologies and statutory guidance.

Training will ensure staff understand online safeguarding risks, including where learners may be particularly vulnerable; appropriate professional boundaries; and their responsibilities for preventing, recognising, reporting and responding to online safety concerns.

Staff will understand the filtering and monitoring arrangements operating within their school, their role within these arrangements and how to report and escalate concerns.

13. Monitoring, assurance and review

CELT will maintain strategic oversight of online safety and review the effectiveness of its arrangements at least annually, and sooner where significant incidents, changes or emerging risks require it, in accordance with *Keeping Children Safe in Education* and relevant DfE standards.

The review will draw on appropriate safeguarding intelligence, including the effectiveness of filtering and monitoring, learner and staff experience, emerging technologies and risks, and relevant local and national information. Findings will inform assurance, continuous improvement and the ongoing development of CELT's online safety arrangements.

Appendix 1 – Learner Acceptable Use Agreement: EYFS/KS1

When I use technology at school:

I will:

- use devices when an adult says I can;
- be kind when I use technology;
- look after school equipment;
- keep my personal information private;
- ask an adult if I am unsure what to do;
- tell an adult if I see or hear something online that worries, frightens or upsets me;
- tell an adult if someone online asks me to do something that makes me uncomfortable; and
- remember that I can always ask for help.

I will not:

- deliberately look for upsetting or inappropriate things;
- share passwords;
- take or share pictures of other people without permission; or
- try to change or bypass school technology settings.

I understand that adults at school help keep me safe when I use technology.

Appendix 2 – Learner Acceptable Use Agreement: KS2

I will use technology safely, responsibly and respectfully.

I will:

- use my own account and keep my password secure;
- protect my personal information;
- communicate kindly and respectfully;
- think carefully before posting or sharing anything;
- ask permission before taking or sharing images of others;
- check whether information online is reliable;
- use AI and other online tools only as directed by school;
- tell a trusted adult if something online worries, frightens or upsets me;
- report bullying, harmful content or unsafe behaviour;
- use school systems and devices for appropriate purposes; and
- follow the school's rules for mobile phones and personal devices.

I will not:

- deliberately access harmful, inappropriate or illegal content;
- share harmful, sexual or humiliating images or messages;
- use AI to create harmful, false or sexualised material about another person;
- bully, threaten, harass or discriminate against anyone online;
- share passwords or access another person's account;
- try to bypass school filtering or security;
- install software or change settings without permission; or
- share school meeting links or access information intended for somebody else.

I understand that use of CELT devices and networks may be monitored to help keep people and systems safe.

I understand that online behaviour both in and outside school may be addressed where it creates a safeguarding concern or has an impact upon learners, staff or the school community through the relevant school policy.

Appendix 3 – Learner Acceptable Use Agreement: KS3–KS5

I understand that access to CELT technology is provided to support education and carries responsibilities.
I will:

- use technology lawfully, safely and responsibly;
- use only my own account and protect my login details;
- respect privacy, copyright and intellectual property;
- communicate respectfully and appropriately;
- protect personal information and consider my digital footprint;
- critically evaluate online information, including AI-generated content;
- use generative AI only in accordance with school expectations;
- acknowledge AI use where required;
- immediately report harmful, illegal or concerning online content or behaviour;
- respect the privacy and dignity of others;
- follow the schools mobile-phone requirements and not use them on site; and
- cooperate with reasonable safeguarding and security measures.

I will not:

- attempt to access another person's account, files or information;
- circumvent filtering, monitoring or security controls;
- access, create, request, store or distribute illegal or harmful content;
- create or distribute sexualised, intimate or humiliating AI-generated images of myself or another person;
- create, share or forward nudes or semi-nudes;
- use technology to bully, intimidate, harass, discriminate against, exploit or threaten another person;
- impersonate another person;
- use CELT technology for gambling, fraud, criminal activity or unauthorised commercial activity;
- record lessons, meetings or individuals without permission;
- share online lesson or meeting links with unauthorised people;
- install unauthorised software or applications; or
- deliberately damage or interfere with CELT systems.

I understand that activity using CELT networks, accounts and devices may be logged and monitored for safeguarding, security and compliance purposes.

I understand that online behaviour both in and outside school may be addressed where it creates a safeguarding concern or has an impact upon learners, staff or the school community through the relevant school policy.

Appendix 4 – Staff Acceptable Use Agreement

As a member of the CELT workforce, I will use technology in a manner consistent with my safeguarding responsibilities, professional role and CELT policies.

I will:

- use CELT-approved accounts, systems and communication channels for professional activity;
- maintain professional boundaries in all digital communication;
- protect passwords and use multi-factor authentication where required;
- lock devices when unattended;
- store CELT information only in approved locations;
- handle personal information lawfully and securely;
- use approved software, applications and AI systems;
- report phishing, cyber-security incidents, lost devices and data breaches promptly;
- report online safeguarding concerns immediately to the DSL or deputy;
- understand and support CELT's filtering and monitoring arrangements;
- supervise learners' technology use appropriately;
- use CELT-approved devices for photographs, recordings or video involving learners;
- comply with copyright and intellectual-property requirements; and
- ensure that my online conduct maintains appropriate professional standards.

I will not:

- use personal social-media or messaging accounts to communicate privately with learners;
- use personal email for CELT business;
- store safeguarding or confidential learner information on personal devices;
- upload personal, confidential, special-category or safeguarding information to an unapproved AI system;
- use AI to make unsupervised safeguarding or other high-stakes decisions about learners;
- deliberately access, create, store or distribute illegal or inappropriate material;
- circumvent filtering, monitoring or security systems;
- access another user's account without legitimate authority;
- install unauthorised software or applications;
- use personal devices to photograph or record learners; or
- undertake online activity which compromises professional boundaries or my safeguarding responsibilities.

I understand that CELT may monitor the use of its devices, networks, accounts and systems in accordance with applicable law and its privacy information.

I understand that breaches may result in restriction of access, safeguarding action, disciplinary action, referral under allegations-management procedures and/or referral to relevant external agencies.

Appendix 5 – Visitor, Volunteer and Contractor Acceptable Use

Anyone provided with access to CELT technology, Wi-Fi, information or systems must:

- use access only for the purpose for which it was provided;
- protect login and access credentials;
- comply with CELT safeguarding and data-protection expectations;
- not attempt to circumvent security or filtering arrangements;
- not access illegal, offensive or inappropriate material;
- not photograph, film or record learners unless specifically authorised;
- report safeguarding or security concerns immediately to an appropriate member of staff; and
- understand that activity on CELT systems may be monitored in accordance with applicable law.

Access may be withdrawn where these requirements are not followed.