



Core Creative Education CIC

CCE014 E-Safety Policy

Explore - Create - Learn – Grow

The purpose of this Policy Statement is to;

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, children and young people and anyone involved in CoRE's activities.

CoRE's E-safety Policy follows legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning.nspcc.org.uk/child-protection-system

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using CoRE's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- *children attending Alternative Provision may be more vulnerable to online exploitation, cyberbullying, grooming, harmful online communities, radicalisation, fraud, coercion and other forms of online harm.*

Artificial Intelligence and AI-Generated Content

CoRE recognises emerging safeguarding risks associated with artificial intelligence, including deepfake images, AI-generated sexual content, impersonation, misinformation, manipulation and online exploitation. Any concerns involving AI-



Core Creative Education CIC

CCE014 E-Safety Policy

Explore - Create - Learn – Grow

generated harmful content will be managed in line with CoRE's Safeguarding and Child Protection Policy.

Nude and Semi-Nude Images

CoRE recognises the safeguarding risks associated with the creation, sharing or possession of nude or semi-nude images and videos by children and young people, including content created or altered using artificial intelligence. Any such concerns will be managed in accordance with current safeguarding guidance and CoRE's Safeguarding Policy.

We will seek to keep children and young people safe by:

- appointing an online safety co-ordinator. CoRE's co-ordinators are Alasdair Green & Sara Bennett
- providing clear and specific directions to staff and volunteers on how to behave online through our staff code of conduct and associated policies together with regular training.
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others. All mobile phones are given to the office when on site. Access to them is only with a mentor and then handed back in again.
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- no mobile phones shall be used on site by staff, volunteers or visitors.
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly *(CoRE uses Linux-based operating systems and network-level filtering systems to reduce access to inappropriate, harmful or unsafe online content. Filtering and monitoring systems are reviewed regularly to ensure they remain effective and proportionate to students' needs.)*
- ensuring that usernames, logins, email accounts and passwords are used effectively. All computers are used alongside a mentor or tutor.
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate. This is kept in a locked office space.
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given



Core Creative Education CIC

CCE014 E-Safety Policy

Explore - Create - Learn – Grow

- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Filtering and Monitoring

CoRE recognises the importance of effective filtering and monitoring systems in protecting children online. Filtering systems are used to reduce access to harmful, inappropriate, extremist, violent, sexual or otherwise unsuitable content. Monitoring systems may be used to identify attempts to access inappropriate content, safeguarding concerns, or behaviour that may place a child at risk.

The Education Manager, Director and Online Safety Coordinators maintain oversight of filtering and monitoring arrangements and will review their effectiveness regularly.

Online Radicalisation and Harmful Content

CoRE recognises that children and young people may be exposed online to extremist, radicalising, violent, hateful or otherwise harmful ideological content. Staff will remain vigilant to signs that a young person may be accessing, sharing or being influenced by such material and will respond in accordance with CoRE's Safeguarding and Child Protection Policy and Prevent Duty responsibilities.

If online abuse occurs, we will respond to it by:

- contacting the school that young person is registered with and having clear and robust safeguarding procedures in place for responding to abuse (including online abuse). Please see Safeguarding and Child Protection Policy. providing support and training for all staff on dealing with all forms of abuse, including bullying/ cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection



Core Creative Education CIC

CCE014 E-Safety Policy

Explore - Create - Learn – Grow

- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance

We are committed to reviewing our policy and good practice annually

Signed: *A Green* (Education manager)

Name: Alasdair Green:

Date 15/7/26

We are committed to reviewing our policy and good practice annually