

Social media and online safety

There are lots of benefits for children and young people when using social media. This includes staying connected with friends and family, enabling innovative ways of learning and creating new ways for them to express themselves.

It can also have many benefits to organisations, for example:

- staying in contact with children outside of face-to-face meetings, activities and events
- providing specialist support to children, such as counselling and therapy
- promoting events
- livestreaming activities
- creating online groups, forums and communities.

But there are risks when you're using social media to communicate with children.

Online risks

Children may be exposed to upsetting or inappropriate content online, particularly if the platform you're using doesn't have robust privacy and security settings or if you're not checking posts. This content might be sexually explicit or it might be harmful in other ways, such as radicalisation, bullying, or content that's upsetting.

Children may be at risk of being groomed if they have an online profile that means they can be contacted privately. Children's posts or profile information may expose personal information and put them at risk. For example, they may talk about their home life, feelings, or thoughts they've been having. There may be information that makes them identifiable such as locations of events they are taking part in or visual clues in photographs. Perpetrators may use this information to groom, abuse or exploit children. Perpetrators of abuse may create fake profiles to try to contact children and young people through the platform you're using, for example an adult posing as a child. They may also create anonymous accounts and engage in cyberbullying or trolling. People known to a child can also perpetrate abuse.

On many platforms, children can be contacted anywhere and at any time through private messaging or notification alerts. This means it's harder for them to escape from abusive messages or upsetting content that they are tagged in. Managing our online presence CIE online presence through our website and social media will adhere to the following guidelines:

- all social media accounts will be password-protected, and at least 2 members of staff will have access to each account and password
- the account will be monitored by at least two designated members of staff in order to provide transparency
- the designated staff managing our online presence (marketing manager) will seek advice from our designated safeguarding lead to advise on safeguarding requirements
- designated staff will remove inappropriate posts by children or staff, explaining why, and informing anyone who may be affected (as well as the parents of any children involved)
- we'll make sure children are aware of who manages our social media accounts and who to contact if they have any concerns about something that's happened online
- identifying details such as a child's home address, school name or telephone number shouldn't be posted on social media platforms
- any posts or correspondence will be consistent with our aims and tone as an organisation
- parents will be asked to give their approval for us to communicate with their children through social media, via video conferencing platforms or by any other means of communication (email, Zoom)

- parents will need to give permission for photographs or videos of their child to be posted on social media (Enrolment form)

- video conferencing sessions will be password protected in order to maintain children's privacy and prevent exposure to inappropriate or harmful content by third parties

What we expect of our staff:

- staff should be aware of this policy and behave in accordance with it
- staff should seek the advice of the designated safeguarding lead if they have any concerns about the use of the internet or social media
- staff should communicate any messages they wish to send out to children to the designated staff responsible for the organisation's online presence
- staff should not communicate with children via personal accounts
- staff should not 'friend' or 'follow' children from personal accounts on social media and maintain the same professional boundaries online as they would in person
- when using organisation accounts staff should make sure any content posted on public personal accounts is accurate and appropriate, as children may befriend them on social media
- rather than communicating with parents through personal social media accounts, staff should choose a more formal means of communication, such as face-to-face, in an email or in writing, or use an organisational account or website
- staff should avoid communicating with children via email or organisational social media outside of normal office hours
- emails or messages should maintain the organisations tone and be written in a professional manner, e.g. in the same way you would communicate with fellow professionals, avoiding kisses (X's) or using slang or inappropriate language
- staff should not delete any messages or communications sent to or from organisation accounts
- staff should undertake all online safety training offered and gain a basic knowledge of the platforms children use and how to report or remove inappropriate content online
- any concerns reported through social media should be dealt with in the same way as a face-to-face disclosure, according to our reporting procedures
- parent are invited to be present during the delivery of any activities via video conferencing platforms at home, but it is not a requirement if it prevents child's natural classroom behaviour
- any delivery of activities to children via video conferencing platforms may be supported by an additional member of staff (even if they're not actively delivering) to ensure transparency
- any delivery of activities to children via video conferencing platforms will be recorded for quality assurance and to ensure transparency
- staff and children must not engage in 'sexting' or send pictures to anyone that are obscene

CIE has the following measures in place

- Child safeguarding policy and procedures
- E-safeguarding policy
- Privacy policy and consent
- Teaching online guidance

Last updated: November 2024

Reporting concerns

Concerns about online abuse or inappropriate behaviour should be reported to:

Simon Llewellyn, Principal

You can also call the NSPCC helpline on 0808 800 5000