Online Safeguarding Policy

Introduction

This policy is intended as guidance for the use of internet and social media by Creswell Heritage Trust and the procedures for safely doing so. It also covers how we expect staff, volunteers and children or young people involved with our organisation to behave online.

Aims

The aims of our online safety policy are:

- The protection of all children and young people who are involved with our organisation and who make use of communications technology (including mobile phones and the internet) whilst engaged with the Trust
- The provision of policy and procedure information about online safety, and responding to incidents, for staff and volunteers
- To ensure our organisation operates in line with our values and mission statement, and in accordance to the law, with respect to our online behaviour

Understanding the online world

When using the internet and social media, our organisation will:

- Understand safety, including acceptable and unacceptable behaviour for staff, volunteers and children, when using online communication and digital media
- Understand that these safety aspects apply irrespective of what electronic devices or channels are being used for communication
- Ensure we adhere to relevant legislation and good practice guidelines in our use of social media (for example Facebook, Twitter, Instagram and TikTok)
- Regular review our safeguarding policies and procedures to ensure that online practice is fully integrated, including the reporting of concerns/disclosures and tackling any instances of online bulling (“cyberbullying”)

Our online presence

Our online presence, whether on the Creswell Crags website, social media platforms, or streaming/conferencing software, will adhere to the following guidelines:

- The Communications and Programmes Manager is the designated responsible person and monitor of the social media presence of Creswell Heritage Trust
- The Learning and Engagement Officer is the designated responsible person and monitor of the digital streaming presence of Creswell Heritage Trust
- All social media accounts will be password-protected, using a strong password with a combination of letters, numerical and where possible special characters
- Passwords should be unique to each user account, to increase security in the case of any external breach
- Users with administrative privileges through their personal accounts (for example Facebook) will follow the password guidance for the organisation with respect to their own accounts
- The designated person managing our online presence will seek advice from the designated safeguarding lead to advise on safeguarding requirements, and in the case of incident reporting
- The designated person will remove any inappropriate content posted by staff, volunteers or children, with an explanation of why this has been done, and communicating with anyone that may be affected
- No personally identifying details, such as address, school name, telephone numbers or email addresses should be posted on online platforms and posts including these details will be removed
- All posts or online correspondence will be consistent with our charitable aims and educational mission
- Users of our social media accounts will be made aware of the responsible person for their management, and given their contact details if they have any concerns
- Parental consent will be sought for any communication with children through social media
- Parental consent will be sought for any photographs or videos of children which may be posted on social media
- Account names and email addresses will be appropriate and up-to-date

What we expect of staff and volunteers

- 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 online communication, including social media and digital streaming
- Staff should communicate to the designated persons any messages they have received from children or young people via social media
- Staff should not “friend” or “follow” children or young people from personal accounts on social media

- Staff should ensure any content posted or streamed is accurate and appropriate
- Staff should not communicate with young people via personal accounts or private messages
- Formal means of communication, such as face-to-face, through organisational emails or in writing should always be used when communicating with children or young people
- A second member of staff should be copied in to any email communication sent to children or young people
- Online communication with children or young people outside of normal office hours should be avoided
- Professional language should always be used, including the signing off of emails, avoiding the use of emojis and symbols (for example “kiss marks” – xx)
- Any disclosures of abuse reported through social media should be dealt with using the same prodedures as face-to-face disclosures, according the the reporting procedures of the safeguarding policy
- Smartphone users should respect the privacy of others and not take or distribute any pictures of other persons without their prior consent
- Staff and young people must not transmit messages or pictures that are obscene, indecent or menacing

What we expect of children and young people

- Children that engage with Creswell Heritage Trust should be aware of this policy and agree to its terms
- We expect children and young people to follow the behaviour guidelines set out in this policy, on all digital devices including computers, tablets, smartphones and consoles

Use of mobile phones

When using mobile phones and other similar devices to communicate, the following precautions will be put in place to ensure the safeguarding of children and young people:

- Staff will avoid possessing the contact details (phone numbers, account handles) of children and young people and instead seek contact through parents or guardians
- On each occasion a child or young person needs to be contacted, parental permission will be sought, identifying the purpose for each contact
- Staff should use a different device from their personal one, for any contact with parents, children or young people
- Texts will be kept to the communication of relevant information as agreed with parents, and not for engaging in conversation
- If a child or young person attempts to engage a staff member in conversation, the following steps will be taken:

- Suggest discussing the relevant information in person on the next occasion rather than continuing remotely
- End the conversation or stop replying

Use of other digital devices and programmes

These principles apply irrespective of what technology is used, or what channel – including any device including computers, laptops, tablets, web-enabled consoles, smart TVs and on social media, through websites, online streaming, online game environments etc.

When digital devices are used within the organisation:

- Children and young people must adhere to the guidelines in our acceptable use policy
- Parental controls will be placed on any devices accessed and used by children and young people, to prevent misuse or harm

As an organisation, we commit to implementing this policy and addressing any concerns quickly and within these guidelines.

Further information and additional resources

The following websites provide information about online safety and how to protect children from harm:

NSPCC/O2 Helpline 0808 800 5002 www.o2.co.uk/help/nspcc/child-protection

Child Exploitation and Online Protection Centre (CEOP)- www.ceop.police.uk

Childnet – www.childnet.com

The UK Safer Internet Centre – www.saferinternet.org.uk