The Wildlife Trust for
Lancashire
Manchester &
North Merseyside

# Online Safety Guidance

## LWT057v1.0

## November 2024

This document is available on the Trust's Intranet site and it should be noted that any printed copies are uncontrolled and may not be the current version of this document.

The Lancashire Wildlife Trust Ltd
The Barn
Berkeley Drive
Bamber Bridge
Preston
PR5 6BY

## Approvals

| Approval | Name | Role | Date |
|---|---|---|---|
| Content | Rhoda Wilkinson | Head of Community Engagement & Designated Safeguarding Lead | March 2023 |
| Quality Assurance | Monica Atherton Patel | Company Secretary | 28/11/2024 |
| Trust Body | Safeguarding Committee | | 15/11/2024 |

The Content Approval denotes that the content of the document has been reviewed and approved by the document owner or their authorised deputy.

The Quality Assurance Approval denotes that this document has been reviewed and approved for conformity with the Lancashire Wildlife Trust QMS. The Document Review Checklist is held within QMS Records.

The Trust Body Approval denotes that if required by the scheme of delegation then the appropriate Trust body has approved the document. Enter 'n/a' if Trust Body Approval is not required.

## Revision History

| Rev. No. | Change Request | Date | Author | Description |
|---|---|---|---|---|
| 1.0 | 32 | 28/11/2024 | Rhoda Wilkinson | Initial Release |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Table of Contents

## 1. Background

The Wildlife Trusts recognise the opportunities and challenges that online engagement bring for the movement, especially those working with and looking to broaden their engagement with children and local communities.

It's easy to see online lives and offline lives as different, but children and young people are growing up with technology and the internet, and for them there isn't a difference; online life and offline life, is just life.

Technology moves at an extraordinarily fast-pace and it can be difficult to keep up-to date with the potential risks and new features of social media, platforms, and apps. While the internet is a fantastic place to learn, create and have fun, as an organisation with an online presence, we have a duty to ensure those engaging with the Wildlife Trusts are equipped to deal with any challenging online safety issues and risks.

## 2. Purpose

The Charity Commission are very clear that operating online carries specific risks that may link to wider Safeguarding issues and organisations must ensure these risks are managed and reflected in policies and procedures.

The purpose of this Online Safety guidance is to ensure everyone involved with The Wildlife Trusts is protected, as far as reasonable possible, from the risks inherent with online engagement.

Staff, volunteers, and trustees must be provided with the information to help keep themselves safe, establish safe online engagement and understand how to respond to incidents, ensuring The Wildlife Trusts are operating in line with our values and the law.

## 3. Online Engagement

Online engagement encompasses all the work The Wildlife Trusts carry out with participants online. These activities are wide ranging and include (but are not limited to):

- Livestreamed public talks and tours
- Facilitated co-production and consultation sessions
- Online chat groups and forums
- Social media engagement
- Website engagement
- Direct e-communications and emails
- Film and photography of participants
- Online education sessions

Platforms for these activities include Zoom, Microsoft Teams, Facebook, Twitter, Instagram, WhatsApp, TIK TOK, Moodle, Discord, YouTube Live amongst others.

## 4. The Potential Risks Associated with Online Engagement

Issues that children may encounter online will vary depending on their age and the nature of their online activities. However, all risks are likely to fall into one of the areas outlined below:

- Children may be at risk because of their own behaviour, for example, by sharing too much information
- Age-inappropriate or unreliable content can be available to children
- Children can be contacted by bullies or people who groom or seek to abuse them
- Potential for inappropriate relationships between adults in positions of trust, or influence and the young people they work with
- Encouragement to take part in violent behaviour or harmful trends
- Young people can be unaware of hidden costs and advertising in apps, games and websites

## 5. Our Commitment Statement for Online Safety

We aim to ensure children, young people and adults are not exposed to online abuse of any kind in their interactions with The Wildlife Trusts; and that we provide all with a positive and uplifting experience.

### 5.1. We recognise:

- The online world provides everyone with many opportunities. However, it can also present specific risks and challenges unique to that environment
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm when interacting with The Wildlife Trusts online
- The online world moves at pace, and we have a responsibility to understand this and the changing nature of the risks that can arise from the different platforms and apps we use
- All children, young people and adults 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 under the Equality Act 2010.
- Working in partnership with children, their parents, carers and other agencies is essential in promoting children's welfare and in helping them to be responsible in their approach to online safety.

### 5.2. We will seek to keep people online safe by:

- Regularly reviewing our online guidance and ensure the guidelines are followed by all those involved in the organisation's online activities
- Providing clear instructions and guidelines to staff and volunteers on how to behave online, and how to safely run online engagement activities
- Ensuring staff and volunteers moderating or involved with online engagement/communities undergo Safer Recruitment Checks as appropriate to their role
- Ensure those interacting with The Wildlife Trusts online understand the behaviour that is expected of them and who they can talk to if they see anything online that causes them concern

- Supporting and encouraging the children, young people and adults engaging in our online activity to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Ensure that popular campaigns such as 30 Days Wild and Nextdoor Nature are monitored closely, and staff understand how to report any concerns
- Ensuring parents and carers understand and give meaningful consent for their children to interact with The Wildlife Trusts online, and that they are signposted to good quality information about the safety features and possible dangers of online communities via websites such as Internet Matters or Thinkyouknow
- Following clear and robust guidelines to enable staff and volunteers 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
- Taking a zero-tolerance approach to the promotion of extremist views, literature, or behaviour
- Ensuring personal information about the children, young people and adults who are involved in our organisation is held securely and processed in compliance with the Data Protection Act 2018 and UK GDPR
- Ensuring that images and film of children, young people and adults are used only after a consent form has been obtained, and only for the purpose for which consent has been given
- Providing induction, support and training for staff, volunteers and trustees about online safety and what is expected from them.

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

- Following our Trusts Safeguarding procedures if the abuse involves children or adults at risk
- Contacting the Police and Local Area Designated Officer if the incident may amount to a crime e.g. online grooming, non-contact sexual abuse, exploitation
- Providing support and training for all staff in dealing with online safety issues
- Making sure our response takes the needs of the person experiencing abuse into account and anyone else who could be affected
- Reviewing national online safety guidance and guidelines at regular intervals, to ensure we continue to learn from the experts and make changes in our practise to enhance our own approach
- Share learning from within the federation, via our Communities of Practice

**To report any Safeguarding concerns or incidents follow the Trusts Safeguarding Procedures.**

# 6. Guidance for staff/volunteers, communicating with children online or via mobile phone

- The purpose of each communication must be clear and in line with the purpose of the Trust
- Ensure all communications are relevant to the work of the group/programme or Trust
- Email and/or social media communications between young people and staff or volunteers should copy in either the parent/carer or another member of the team

- Only use Trust email accounts or Trust social media platforms (if this isn't possible, managers can authorise individual staff and volunteers to use a personal device on a case-by-case basis and keep a record of this authorisation and who can see the communication)
- Never provide personal contact details/social media details or personal email addresses and it is best practice advice not to accept friend requests from children and families engaging with The Wildlife Trusts
- Do not use language that is directly (or could be misinterpreted as being) racist, sexist, derogatory, threatening, abusive or sexualised in tone in any communication
- Ensure communication and the methods used e.g. platform or community are age-appropriate for the group
- Ensure children understand what is expected of them communicating online using a code of conduct (you could encourage participants to co-create this with staff/volunteers) and that they know who they can talk to if they have any concerns or see something online that worries them
- Texts, emails or messages will be used for communicating information – such as reminders about upcoming events, changes of plan due to weather etc and not to engage in a conversation. If a child misinterprets such communication and tries to engage a staff member in conversation, the staff member is advised to:

    - Stop replying and suggest discussing further at the next meeting
    - Inform line manager in the interests of transparency
    - Contact the Trusts Designated Safeguarding Lead, if there are concerns for the child
    - Signpost the child to someone appropriate they can talk to

- If any allegation is made against a staff member or volunteer regarding their conduct online, this must be reported immediately to the Trust's Designated Safeguarding Lead.

## 6.1. Online Community/Platform considerations

It's challenging how to decide which online platform to use when you're wanting to build a virtual community or share ideas and make plans between a group. Here is a list of considerations to be mindful of when making a choice:

- Age – most platforms will have an age restriction so make sure you're not asking children to sign up to a platform they may not be old enough to use (e.g. Facebook is 13, WhatsApp is 16, TikTok is 13 and Snapchat is 13)
- For children under 16, make it clear in group/programme consent forms which online platforms are used to support the group and suggest parents/carers familiarise themselves with the platform and the safety features
- Don't chose a platform where 'live location' cannot be turned off – meaning anyone who views posts, can see the exact location of posts and potentially where children or other vulnerable groups meet
- Be clear with members about expected behaviour and consequences for those breaking these (please see example code of conduct in appendix). It's helpful to pin a reminder code of conduct on a page within the group that is easily accessible and write the code of conduct with the active participation of members
- As part of a welcome session where users are demonstrated functionality, draw attention to safety features within the platform/app (e.g. report, block, accessibility, displaying personal information etc)

- Identify Trusted Adults - ensure young people in your care would know what to do and who to talk to if something they see while using any app makes them feel uncomfortable and revisit this topic on regular occasions

## 6.2. Posting videos/images online

Sharing photographs and images online carries potential risks e.g. people (particularly children) can become vulnerable to grooming if personal details are shared alongside images that makes them identifiable, images can be copied, shared or downloaded by anyone and images of children can be adapted and used inappropriately. Once an image is out there, it's out of our control and can be downloaded, screenshotted or shared by anyone. There is potential for comments to be made on photos and videos that can be hurtful and detrimental to people's wellbeing.

**Before sharing any images online consider:**

- Images are taken and saved securely on Wildlife Trust equipment (never on personal devices)
- The purpose and why the image is being used
- Do you have written consent from parents/carers, or the person themselves if over 16 years old
- How widely the image may be shared
- The post doesn't contain any personal or identifiable information being shared with the image e.g. name and visible school uniform logo
- Live location is turned off

If the person or parents/carers do not consent to photographs being taken or shared online, their wishes must be respected. It should be agreed in advance how they would like to be identified so photographers understand not to take photographs of them and ensure this is done in a sensitive way that doesn't make them feel singled out or embarrassed.

**Storing images securely**

If images or video recordings are being stored for Trust use, you must ensure compliance with the Data Protection Act 2018. This means taking steps to ensure they are stored safely. This includes:

- Only store images and video in a Trust managed storage service which encrypts data at rest and in transit
- Set permissions to restrict access only to those who need it
- Ensure the images and video are only kept as long as needed, and in compliance with your data retention policy
- Ensure anyone taking photos and videos has the correct permission to do so and are recruited in line with safer recruitment best practise e.g. consider if the role is eligible for references and DBS checks

# 7. Appendix

## 7.1. Appendix 1 Example Online Code of Conduct

**Example Online Code of Conduct for all *(best practice advice is to co-create one with group participants using these guidelines as a base and age-appropriate language for the group):***

The Trust wants to provide a positive online experience for all.

This means free from harassment, bullying and hate. Our online spaces should be safe and welcoming for all our participants and everyone joining us has a responsibility to work with us to achieve this.

This code of conduct outlines our expectations for everyone's behaviour as well as what will happen to those showing any unacceptable behaviour. All staff and participants are required to agree to the following code of conduct to ensure a safe and secure environment for everyone.

**Expected behaviour for all:**

- To be considerate, respectful, and work together with all group members
- Not to use unpleasant, unfair, or un-kind behaviour and speech
- To respect differences in opinion and values
- Be mindful of your fellow group members – listen and allow time for other people to speak
- Be mindful to stay relevant to the purpose and aims of the session

**Technical guidance for all:**

- Do not share any personal details with others or your live location (e.g. last names or where you live)
- Please mute yourself if there is background noise
- If asked, please add your first name only
- If you are sharing your screen by mindful of what else might be in your background or give away personal details such as where you live

We will not tolerate harassment or bullying of any kind and anyone showing those kinds of behaviors will be asked to leave or removed by the organiser.

If you have any concerns regarding the actions of any other users, please notify a staff member immediately so that we can help you.

*If you regularly engage with children online you may wish to go one step further and create an 'online safety agreement' with those you're working with. Click here to see the guidance from the NSPCC and a sample statement.*

## 7.2. Appendix 2 Online Guidance for Staff, Volunteers or Trustees

In your role, you are acting in a position of trust and have a duty of care towards the people we engage with online. You are likely to be seen as a role model or in a position of authority and are expected to act appropriately and model good behaviours.

**Good Practice for Virtual Communities**

- Ensure that whenever possible, there is more than one adult present during online activities with children, young people and adults at risk. If a situation arises where you are alone with a child, young person or adult at risk, for example in a virtual session, ensure that you are within sight or hearing of other adults.
- Avoid giving personal contact details (e.g. personal mobile number, personal email or private social media account) to members of the public, volunteers or supporters.
- Provide a safe online environment for children, young people and adults at risk which provide clear ground rules and participants know who they can talk to if they have a concern
- Create a code of conduct that all participants agree to
- Ensure IT equipment, including mobile devices, is used safely and for its intended purpose.
- Have good awareness of issues to do with safeguarding and child protection that may arise online and act when appropriate.
- In the event of an incident, follow policies and procedures for safeguarding, whistleblowing and online safety.
- Understand that children, young people and adults are individuals with individual needs. Respect differences in gender, sexual orientation, culture, race, ethnicity, disability and religious belief systems, and appreciate that all participants bring something valuable and different to the group/organisation.
- Challenge any unacceptable behaviour, including discrimination and prejudice, and ensure that participants understand this will not be tolerated
- Encourage a safe space where children, young people and adults can speak out about attitudes or behaviour that makes them feel uncomfortable.
- Consider the long-term implications of content posted online, and exercise caution when you are discussing sensitive issues with children, young people or adults at risk e.g. climate change and wildlife and species decline
- Promote relationships that are based on openness, honesty, trust and respect.

## 7.3. Appendix 3 Hosting live online events

When hosting a live event, it is important to consider the safety of your target audience as well as staff, volunteers and potential speakers.

There are a number of different platforms available such as Zoom, Facebook, MS Teams etc. and you need to consider the audience you are intending to reach and which is the most suitable platform e.g. is it a livestream broadcast, a small webinar with a restricted audience or if you want to facilitate audience involvement and participation. Some points to help guide your choice include:

- Intended audience? Are they allowed to use the platform you have chosen – for example Facebook and Zoom have age restrictions of 13 and 16 respectively
- If audience participants are under 16 then you must gain consent (consider building this into consent forms as part of the wider group or programme)
- Consider whether your audience has access to the platforms – have you checked they have accounts and can use them?
- Provide clear and simple instructions of how to join and participate
- Prepare in advance
- Are you confident in sharing your screen and displaying content without giving away information you don't want to share (e.g. personal information, your emails etc)
- If there will be children or young people present consider how they will be supervised during the calls e.g. do you want parents or carers to remain in the room, do you request calls take

place in a shared space such as the living room and ensure this is included in your consent forms allowing them to take part

- Run through your code of conduct at the beginning of each session as a reminder and encourage everyone to consider their content and language – particularly if younger children are present
- Remind participants of the functions within the platform e.g. how to raise your hand, report any concerns to a host privately and if you are recording the session make viewers aware
- If the event is public and you cannot verify audience members be clear about this with participants and ensure they know who to contact at your Trust if they have concerns about another participant
- Be aware that hackers may utilize live events – do you know how to shut down the event if you needed to?

**Ensure you have the capacity to manage the event safely**

- Try to have at least two members of staff or volunteers available to support and manage a live event. One to present and one to manage the chat and provide support.
- If you are utilizing some of the break-out rooms functions of different platforms such as Zoom or MS Teams, try not to be left alone with a child or young person (just as you would working face to face)
- Have a 'Plan B' in place in case your event is disrupted or hacked – the best course of action here is to shut it down and reschedule, rather than attempting to continue – this demonstrates your commitment to keeping everyone safe and that you will not tolerate inappropriate behaviour. You can contact participants afterwards to explain your course of action and set up another date
- If users are being purposefully disruptive or actively 'trolling' on a public Trust page or site such as Facebook – it is usually better not to engage or interact with them and report them to the user or platform admin team instead.