Wiltshire Wildlife Trust

A future where wildlife and people flourish in harmony

Online Safety Policy

This policy should be read in conjunction with the following associated documents:

- Wiltshire Wildlife Trust Safeguarding Policy and procedures.

- The Wiltshire Wildlife Trust staff handbook.

- Staff conduct policy

Purpose

Wiltshire Wildlife Trust (WWT) recognises the opportunities and challenges that online engagement may bring for staff and those working with children, young people and adults at risk. For many, particularly younger generations, online and offline life are seamless, and it is essential that we adapt to this reality when delivering services and activities.

Technology evolves rapidly, and keeping up with emerging risks and new features of platforms can be challenging. While WWT does not assume responsibility for an individual's online safety outside its operations, we do have a duty to ensure that all children, young people, and adults at risk engaging with us are safeguarded during online interactions facilitated by our organisation.

This policy provides overarching principles to guide our approach to online safety within WWT's activities. It applies to all staff, volunteers, and trustees working on behalf of WWT. When WWT collaborates with third parties, staff must review and adhere to the third party's policies where applicable, ensuring they align with WWT's safeguarding standards.

Digital engagement

Digital engagement encompasses all the work carried out with participants online. These activities are wide ranging and may include:

- Live-streamed 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

Digital platforms for these activities may include Zoom, Microsoft Teams, Facebook, WhatsApp, X (formerly Twitter), Instagram, TikTok, BlueSky, Moodle, Discord, YouTube Live among many other platforms.

Online safety is the process of limiting the risks to children, young people and adults when using the

internet, digital and mobile technology.

We believe that:

- Children, young people, and adults should never experience abuse of any kind.

- Children, young people and adults should be able to use the internet for learning, enjoyment and personal development, but safeguards and guidance need to be in place to help ensure they are kept safe.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present specific risks and challenges unique to the internet

- We have a duty to safeguard all children, young people, and adults involved in our organisation are protected from potential harm during online interactions facilitated by WWT

- The online world is forever evolving; we have a responsibility to understand this and the changing nature of the risks that can arise from different apps, platforms, and methods of online communication

- 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

- Working in partnership with children, young people, adults at risk, their parents, carers and other agencies is essential in promoting their welfare and in helping them to be responsible in their approach to online safety.

We seek to keep people safe online 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, volunteers and trustees on how to behave online, and how to run online engagement activities as safely as possible

- Supporting and encouraging the children, young people and adults engaging in our digital activity to use the internet, social media and mobile phones in a way that helps to keep them safe and shows respect for others

- Ensuring that popular campaigns with lots of digital engagement, such as 30 Days Wild, are monitored closely and staff understand how to report any concerns

- Supporting and encouraging parents, educators and carers to do what they can to keep those in their care safe online

- Following clear and robust guidelines 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

- Ensuring personal information about the children, young people and adults we are working with online is held securely and managed according to the UK GDPR regulation

- Ensuring that usernames, logins, email accounts and passwords are used effectively

- Ensuring that images and video of children, young people and adults at risk 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 and volunteers

- Risk-assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse is suspected have occurred, we will respond to it by:

- Following our Safeguarding Procedure if the abuse involves children or adults at risk

- Providing support and training for staff working online with children and adults at risk in dealing with all forms of digital abuse

- Making sure our response takes the needs of the person experiencing abuse, any witnesses or bystanders, and our organisation as a whole into account

- Reviewing the Online Safety Policy and guidelines annually, in order to ensure that any problems have been resolved in the long term, we learn from practice and embed any changes needed to enhance our online safety.

> To report any online safety or safeguarding concerns and incidents, follow guidance in the relevant Wiltshire Wildlife Trust **Safeguarding Procedures for Children or Safeguarding Procedures for Adults at Risk**.

Social media guidance for staff

- The use of social media can have many benefits, such as greater opportunities to showcase and amplify our work as well as reach wider audiences who may choose to support us.

- WWT understands that many employees will maintain their own personal social media accounts and this overview is designed to help employees to use social media effectively, while protecting the independence and reputation of WWT, and preventing any potential issues that may arise.

- In line with guidance from across the sector, if staff list WWT as their employer on personal social media platforms they should also post a disclaimer e.g. "views expressed are my own", "all opinions are my own", or words to that effect.

- Staff and volunteers should be aware of their digital footprint. Children, young people and supporters may look up the personal social media accounts of people who are working with them so these should be free of inappropriate or harmful content and not provide any personal information such as personal email addresses or phone numbers.

WWT encourages staff, volunteers and trustees to get involved in media posts and campaigns in the following ways:

- Liking and commenting on our social media posts

- Sharing our posts, stories, and information about live events or campaigns

- Creating your own posts about your work or our work, e.g. #WilderKent

WWT Online Safety Policy – Reviewed and adopted 26 January, 2026

All staff using social media in their role with WWT or reflecting an association with WWT on their personal social media accounts must do so in respect of the following guidance:

- Social media is a place where people can have conversations and build connections. Other people may have different values, customs and viewpoints and it is important to respect those. When interacting with people on social media do not post any content that is considered to be offensive, discriminatory, demeaning, abusive, threatening, defamatory or inappropriate.

- Employees should only comment within their own area of expertise to provide individual perspectives on non-confidential activities.

- Employees should seek guidance before participating in social media when the topic being discussed may be considered sensitive (e.g. reintroducing species, use of pesticides etc. which may have reputational impact). Social media activity around sensitive topics should be managed by the Communications Team within the Engagement and Fundraising directorate.

- There may be instances whereby WWT require staff to remove social media posts which they feel constitute a breach of the standards outlined and this could also amount to disciplinary action as per the staff handbook.

- Should any members of staff be alerted to negative content regarding another member of staff they should notify their line manager or HR immediately.

- Be vigilant with your social media security – change passwords regularly, turn on two-factor authentication, review your privacy settings and consider who can view your content and posts.

Practical guidance when using social media

- Do not use the WWT logo or promotional/campaign materials without permission – unless you are re-posting from official accounts.

- Do not use any other organisation logos, brand names, trademarks or slogans without permission to do so.

- Do not use images, videos or quote any staff, or partners without their consent to do so.

- Be aware that sometimes information our staff are privy to is sensitive or under embargo – be sure to only share information you have the permission to

If you have any questions regarding social media, please speak to the Trust's Communications Team who can offer further guidance.

Online communities and platforms

If there is a need to create a virtual community, space to share ideas, or a place to plan with others, it's important to carefully consider and plan. Take into account the following considerations:

- Age – most platforms will have an age restriction, check that you're not asking children to sign up to a platform they may not be old enough to use (e.g. Facebook, Snapchat and TikTok is 13yrs and WhatsApp was changed to 13yrs from 16yrs in April 2024 etc.).

- For children under 16, make it clear in your group consent forms which online platforms you use to support the group and suggest parents/carers familiarise themselves with them and the safety

features. Websites such as **thinkyouknow.co.uk** or **saferinternet.org.uk** are helpful to signpost parents and carers to.

- Don't choose a platform where you can't turn off 'live location' – meaning anyone who views posts, can see your exact location.

- Ensure you are clear with members about expected behaviour and consequences for those breaking this (see Appendix 1: Example Code of Conduct). It is helpful to 'pin' the Code of Conduct on the front page within the group that is visible and easily accessible.

- As part of a welcome session where users are shown 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. Revisit this topic on regular occasions.

- Ensure parent/carer permission has been obtained and that information has been shared on the purposes of the online community/platform including sharing staff contact details.

- Ensure staff that are supervising groups have been safely recruited and are DBS checked.

Posting images and video online

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

Before sharing any images online consider:

- The purpose and why the image is being used

- If written consent has been obtained from parents/carers or the person themselves if over 16

- How widely the image may be shared

- The post doesn't contain any personal or identifiable information being shared with the image (use a false name if necessary)

If the person or parents/carers do not consent to photographs being taken or shared online, we must respect their wishes. It will 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 WWT use, you must ensure compliance with the Data Protection Act 2018. This means taking steps to ensure they are stored safely. This includes:

- Storage within a safe location

- Password protecting or encrypting electronic images before they are stored

- Only using devices belonging to WWT to take and store images or videos

- Ensure anyone taking photos and videos has the permission to do so and has the correct level of DBS certification to undertake this task, whether volunteer or a member of staff.

- The use of protected WhatsApp groups to share images among staff within departments is acceptable but these should only be images with agreed consent or photos that do not require consent i.e. photos that do not contain images of children, young people or adults at risk. These WhatsApp groups should all contain a member of the Comms Team who will monitor the images and can advise on their use.

- Images and video should be transferred on to the Trust's protected SharePoint site for images and permissions need to be retained for a minimum of 5 years. Access to images will be restricted to staff and all images and videos must only be used for the purposes given on consent.

- Staff must delete images and videos from all systems once permission has lapsed.

Further information on photography and filming of children and adults at risk can be found in the Trusts **safeguarding procedures for children and safeguarding procedures for adults at risk.**.

Wiltshire Wildlife Trust's Safeguarding Team

Damian Haasjes – Director of Education and Wellbeing – Safeguarding Lead
T: 07793 251558 | E: damianh@wiltshirewildlife.org

Dean Sherwin – Head of Care Farms
T: 07887 758380 | E: deans@wiltshirewildlife.org

Gail Grimes – Head of Youth, Education and Wellbeing
T: 07736 457649 | E: gailg@wiltshirewildlife.org

Ali Nott – Engagement Manager
T: 07849 089875 | E: alin@wiltshirewildlife.org

Becki Mckinlay – Director of Fundraising and Engagement
T: 07597 589587 | E: beckim@wiltshirewildlife.org

Imogen Jackson – Adult Wellbeing Manager
T: 07702 802961 | E: imogenj@wiltshirewildlife.org

WWT Safeguarding Phone: 07849 085423

Appendix 1: Example Code of Conduct

Wiltshire Wildlife Trust want 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 help 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, volunteers 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 participants

- Not to use unpleasant, discriminatory, or harassing behaviour and speech

- To respect differences in opinion and values including political, religious, and other views

- Be mindful of your fellow participants – 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 prompted, please add your first name only

- If you are sharing your screen, be mindful of what else might be in your background or give away personal details

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

If you witness or experience harassment or have any concerns regarding the actions of any other users, please notify a staff member immediately so that steps can be taken to keep you safe.

If you have any concerns or would like a confidential discussion, please contact the Safeguarding Lead via the details below:

Damian Haasjes – Director of Education and Wellbeing – Safeguarding Lead
T: 07793 251558 | E: damianh@wiltshirewildlife.org

Wiltshire Wildlife Trust

A future where wildlife and people flourish in harmony

Appendix 2: Online Guidance for Staff

In your role you are acting in a position of trust and have a duty of care towards the children, young people, and adults you 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 behaviour. Please read the following guidance before engaging online:

- Provide as safe an online environment as possible for children, young people and adults at risk which provide clear ground rules (see code of conduct above).

- Ensure IT equipment, including mobile devices, are used safely and for their intended purpose.

- Have good awareness of issues to do with safeguarding and child protection and take action when appropriate.

- Follow policies and procedures for safeguarding, whistleblowing and online safety.

- Treat children and young people fairly and without prejudice or discrimination.

- 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.

- Challenge all unacceptable behaviour, including discrimination and prejudice, and report any breaches of this behaviour code to the Safeguarding Lead.

- Encourage a safe space where children, young people and adults can speak out about attitudes or behaviour that makes them 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.

- Promote relationships that are based on openness, honesty, trust and respect.

- 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.

- Do not give personal contact details (e.g. personal mobile number, personal email or private social media account) to members of the public, volunteers or supporters.

Guidance for communicating with under 18s

- Anyone working with children, online and offline, should follow Safer Recruitment practices, to help ensure our staff and volunteers are suitable to work with children

- Ensure you have completed safeguarding training and have had a DBS check

- Signed parental/carer consent should be given prior to email, social networking and mobile phone communications with under 18s

- If any specific digital platforms are being used to facilitate groups in addition to texts/emails e.g. Discord, TikTok or WhatsApp, this should be made clear within the consent and parents/carers signposted to further information about them via websites such as NSPCC, UK Safer Internet Centre, National Crime Agency or Internet Matters

- The purpose of each communication must be clear

- Ensure all communications are relevant to the work of the group/programme or WWT

- Email and/or social media communications between young people and staff or volunteers should copy in either the parent/carer or another member of staff

- Use WWT email accounts or WWT 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 do not accept friend requests from children and families we are engaging with

- 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 is age-appropriate

- Ensure children understand what is expected of them communicating online using a code of conduct and that know who they can talk to if they have any concerns or see something online that worries them

- If any inappropriate communication or content is alleged or shared between an adult staff member or volunteer and a child (under-18-year-old), this must be reported immediately to the Safeguarding Lead.

Wiltshire Wildlife Trust

A future where wildlife and people flourish in harmony

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, Microsoft 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 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 13yrs and 16yrs respectively

- If audience participants are under 16yrs 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, sensitive organisational communication e.g. Teams notifications etc.)

- If there will be children or young people present, give consideration to 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 how to contact the organiser/Safeguarding Lead if they have concerns about another viewer

- Be aware that hackers may utilise live events – ensure 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 using break out rooms, 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 WWT 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.