Social Media Policy (2023)

Document Control

Document name	Social Media Policy
Original file path	210713 Social Media Policy AW.docx
Author(s)	Abi Webber with input from Catherine Day and Becky Fisher
Version	1.7
Date published	March 2022

Policy Details

Review frequency	Annual
Previous review date	November 2021
Date of next review	November 2022
Approval level	Council
Date approved	
Responsible Director	Catherine Day
Responsible Trustee(s)	
Is this policy required to enable the Trust to meet statutory or legal requirements?	Yes
Committee(s) responsible for review	Safeguarding, GDPR, IT, Fundraising, HR
Committee(s) responsible for monitoring compliance	Safeguarding, GDPR, IT, Fundraising, HR

Audit History

Version	Date	Summary of changes/updates	Revised by:
1.0	Feb 2019 - Draft started following discussion in Safeguarding Committee Meeting	Agreed a Social Media Policy is required for the Trust to support the Safeguarding and Child Protection Policy, as well as guiding staff on the use of social media at work, as this is increasing in many staff members' work capacity. Cyber bullying was mentioned as an important area for inclusion.	Abi Webber
1.1	18th March 2019	Amendments made following consultation with Alison Fowler, Natasha Thorneloe and Hannah Terry. Updates include: Clarification in wording of '4.1 Responsible use of Social Media' and creating a Code of Conduct (Annex C) Clarification in wording and seriousness of sections '4.2 Cyberbullying' and how it links to other Trust Policies.	Abi Webber
1.2	1st April 2019	Amendments made following consultation with Alison Fowler, Natasha Thorneloe and Hannah Terry. Updates include:	Abi Webber

		Clarifying duties of staff (4.3) and the boundaries between personal and professional use; Updated section 6. Training, Governance and Policy Review	
1.3	30th April 2019	Following safeguarding committee meeting: - Clarification and tweaks to wording about what is classed as inappropriate conduct on social media with regards to talking about stakeholders. - Adding the whistle blowing procedure as an option in the reporting of cyberbullying section	Abi Webber
1.4	14th June 2019	Following Exec Team review: - The Trust's guidance on using Twitter added to the policy as an appendix. - The policy's section on posting on social media changed to provide greater clarity to staff on how they should use both personal and work social media accounts including "liking" posts made by others that could be seen as controversial or inflammatory. - Rather than covering all of the Trust's volunteers (because there are so many and managing this would be problematic), the policy will apply to those volunteers with defined roles with the Trust such as Local Group members, Trustees and Ambassadorial positions, e.g. Marine Champions.	Abi Webber
1.5	10th March 2020	- Updating a few typos within the document and the legislation page. The Data Protection Act 1988 was superseded by the Data Protection Act 2018, and the Malicious Communications (NI) Order 1988 is not relevant to us.	Abi Webber
1.6	1 November 2021	- Updated Designated Social Media Leads to Elenya Lendon, Catherine Day and Hannah Terrey. - Section 4.3 under safeguarding compliance - wording around the use of images updated to allow staff/volunteers to share images of people if the correct permissions have been granted. - Section 4.4 and Annex c updated to include '*posting abusive content, "adult" content, illegal content, offensive content, discriminatory content and racist language would result in disciplinary action*'.	Abi Webber, Elenya Lendon, Catherine Day
1.7	4 March 2022	-Addition to 4.3 creating a safe environment to include guidelines for communicating with children and adults at risk online.	Becky Fisher, Catherine Day

Contents

1. Introduction

Hampshire & Isle of Wight Wildlife Trust uses social media for brand awareness, education, engagement, fundraising and campaigning.

This social media policy is for all Trust staff, volunteers* or contractors who create or contribute to social networks, blogs, wikis, or any other form of e-communications for authorised work purposes using the Trusts brand.

As staff and volunteers use social media for personal use during working hours and for work use during out of work hours, the use of social media can distort where the boundaries are between home and work.

The policy has been created with the intention to empower staff to use social media to represent the Trust, and to engage with social media at a level at which they feel comfortable. It is important that everyone approaches the social media world in the same way they do the physical one - using sound judgment and common sense and adhering to the Trust's values, code of conduct and all applicable policies.

** This policy applies to volunteers with defined roles within the Trust such as Local Groups, Trustees and Ambassadorial positions e.g. Marine Champions.*

2. Policy scope

The Trust recognises that social interaction online is an important and integral part of life and, if used correctly, can offer valuable professional opportunities. However, inappropriate use of social media can be a serious drain on productivity, pose a significant safeguarding and organisational risk and impact on staff morale.

This policy is for all Trust employees, trainees, volunteers or contractors who create or contribute to social media. It is intended to:

- Ensure that staff understand the extent to which personal use of social media is permitted during hours of work;
- Provide guidance on when and how to use social media for work purposes;
- Protect the Trust's brand, staff and volunteers, including preventing and dealing with complaints or cyberbullying;
- Protect the public and, in particular, safeguard the welfare of children and vulnerable adults in relation to the Trust's use of social media.

3. Definitions of key terms

For the purpose of this policy, when the term 'staff' is used, it should be assumed this refers to staff AND volunteers AND contractors.

For the purposes of this policy, 'social media' is the term used for internet-based tools used on computers, tablets, and smart phones to help people keep in touch and enable them to interact instantly with each other, or to share data in a public forum.

This includes channels such as Twitter, Facebook, Instagram, Pinterest, Flickr, YouTube, Wikipedia and LinkedIn as well as blogs. In some areas, such as online bullying, this also includes use of emails, WhatsApp and text messaging.

Employees should be aware that there are many more examples of social media than can be listed here, and this is a constantly changing area. It is expected that anyone who participates in any form of social media on behalf of the Trust understands and follows this policy.

4. Policy details

4.1 Responsible use of social media

The Trust understands and encourages staff to participate on social media on behalf of the Trust in work hours, for legitimate purposes. However, this must be done properly, and staff must exercise sound judgment and common sense to prevent social media from becoming a distraction at work.

Whether you are speaking "on behalf of the Trust" or speaking "about" the Trust, all staff must adhere to all applicable Trust policies and Social Media Code of Conduct (Annex 3). Staff must be accountable for their own actions; anything posted that can potentially harm the Trust's brand will ultimately be their responsibility.

The Trust respects the free speech rights of staff, however staff must be cautious when mixing professional and personal lives online, as these are likely to intersect. It is important to remember that stakeholders, partners and the public may have access to all online content that is posted, not just that that is intended for work purposes.

Staff must be aware of how their behaviour on social media can impact the Trust, even when they are not posting in a work capacity, but on their personal accounts. Staff must use common sense and sound judgement and be aware that even on personal accounts they are representing the Trust. Once a post has been shared online it becomes public record. As well as writing posts this also included liking and sharing posts created by others which could be seen as controversial or inflammatory,

Inappropriate conduct on social media could include negative comments about employees, members of the public and the employer, or abusive comments towards stakeholders, bringing the organisation into disrepute or a breach of confidentiality (unauthorised disclosure of charity information) e.g. details relating to financial accounts, redundancies, employee personal information, details of grievances/internal complaints. This also includes breaching our charity and regulatory duties such as showing overtly party political opinions. See Annex A, B and C for details.

4.2 Cyberbullying and harassment

Cyberbullying or harassment can be defined as:

> *Any unwanted conduct which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment.*

Full details of what constitutes cyberbullying are outlined in ***Annex A: Types of cyberbullying.***

Online bullying and harassment could take place on any digital device such as mobile phones, tablets, laptops and desktop computers. It could occur on social media, website forums/comments, blogs, apps, videos, emails or text messages.

The Trust is committed to providing all staff with a safe and civil working environment in which all employees are treated with dignity and respect. Any form of cyberbullying or harassment by staff is totally unacceptable, and no form of intimidation, bullying or harassment will be tolerated.

If a complaint of harassment or bullying is brought to the attention of management, it will be investigated promptly and appropriate action will be taken.

For more information please refer to the Staff Handbook and Harassment and Bullying Policy.

Reporting incidents of cyber bullying

Anyone who feels they are being subjected to cyberbullying must speak to a Senior Manager or a member of HR immediately.

Anyone who suspects someone else of carrying out cyberbullying or experiencing cyberbullying must speak to a Senior Manager or a member of HR immediately.

If you feel uncomfortable talking to a Manager or HR, or you feel the behaviour is continuing and nothing is being done, you can also look at the whistle blowing procedure.

The Trust will ensure that all allegations of cyberbullying are handled and investigated appropriately. It may be possible to resolve matters informally, as people may not be aware that their behaviour is unwelcome and, during an informal discussion, an agreement may be reached that the behaviour will stop.

If an informal approach is not possible, the Trust can decide that the matter is a disciplinary issue, which will need to be dealt with formally.

Any incident of such a scale or nature which poses a potential reputational risk to the Trust should be handled in accordance with the Trust’s Serious Issue Procedure.

The Trust will also provide information on the Trust’s website to ensure that members of the public have a mechanism for reporting concerns.

Cyberbullying incidents that involve children or vulnerable adults must also follow the guidance set out in the Safeguarding and Child Protection Policy, and be reported to a Designated Safeguarding Lead immediately.

4.3 Creating a safe environment

It is the responsibility of both the Trust and staff to use technology safely and appropriately.

Duties as an employer

- Ensure adequate firewalls are in place to prevent inappropriate content coming into or going out of the Trust.
- Ensure web security tools are in place to monitor or restrict usage and prevent access to specific websites.

- Ensure spam prevention tools are in place to block emails containing inappropriate content reaching employee's inboxes, and ensure they cannot be sent onwards from employee's email systems.
- Provide antivirus software to detect, prevent, and take action to disarm or remove malicious software programs, such as viruses and worms.
- Provide staff with relevant guidance, training and updates in the use of social media at work.

Duties of staff

The boundaries between the personal and professional use of social media are hard to define. The Trust expects staff to always use the highest level of guidance set out in this Policy when using social media.

- Staff are allowed to make occasional personal use of social media while at work, using the Trust's IT or communication resources and equipment, as long as all use complies with this policy and does not interfere with their performance of work duties.
- Staff must ensure that all media enquiries and requests for comments on social media are directed to the Communications Team.
- Ensure high restriction levels in privacy settings on social media sites have been set.
- Staff must make sure they understand a website's terms of service.
- Staff need to protect access to all channels through the use of strong passwords.
- Be vigilant, and do not use or align the Trust with any organisations or websites that deploy the use of excessive tracking software, adware, malware or spyware. These should be blocked by firewalls and web security tools, but may occasionally get through.
- Do not attempt to access websites on the computer and/or phone that have been restricted by the Trust. If a website will not open then do not try and find a way to access it.

- Safeguarding compliance:
  - On personal profiles, staff must not post images of members of the public or event participants taken during work-related activities, where the individuals can be identified, unless the social media account can be clearly linked with the promotion of Trust activities and the correct model release permissions have been granted. Photography cannot be shared in a personal capacity otherwise.
  - Volunteers must sign the Trusts *Volunteer Social Media and Photography Agreement* if using images on social media to promote the Trusts work.
  - Where photography permissions have been gained it is important to remember this declaration is for use by the Trust rather than by individuals. This is particularly important in relation to under 18s and vulnerable adults for safeguarding reasons.
  - When posting images of people ensure that the correct permission has been granted – **see the photography permission procedure for full details** on this process.
  - Relationship forming – do not form a new relationship with anyone on a social media platform e.g. do not accept friend requests from people you do not know. Keep all contact professional and do not engage in personal conversations e.g. discussing dating.
  - If you feel that a member of the public is trying to develop a personal rather than professional relationship with you across social media, stop communications straight away and speak to a Designated Safeguarding Lead.

Additional guidelines for communicating with children or adults at risk online

- Online communication should be conducted in the same way you conduct face to face communication and is considered the same for safeguarding and child protection purposes. Apply the principles of the Safeguarding and Child Protection policy, and those set out within the rest of this policy.

- Only use verified Trust communication channels, or your work email or mobile phone to communicate with children or adults at risk.

- If communicating with influencers online who are under 18 ensure your messages are publicly available, i.e., use replies and comments rather than direct messaging. If using a personal account, ensure you identify yourself as a member of Trust staff.

- Wherever possible, communication with a child or adult at risk should be conducted through their parent, guardian or carer.

- Where direct communication with children or adults at risk is required, this should be approved by your line manager, in consultation with the Designated Safeguarding Lead and a member of the communications team. You should not set up any new online groups or communication methods without approval. All communication methods or online groups specifically designed for children or adults at risk will be listed on the review of education and engagement activities and reviewed annually inline with the Safeguarding and Child Protection reporting.

- Working with the DSL and communications team, the following should be considered before setting up a communication group for children or adults at risk:

    - How will you provide information to parents, guardians and carers and gain their consent?
    - Is it possible to include parents, guardians or carers within the group? Is this appropriate for the age group you are working with?
    - How will you create a closed group and verify the identity of members?
    - Which platform is the right one for your group? Are their age restrictions on the platform you'd like to use? Is the platform used by the age group you are working with? Will members of the group be able to see contact information for others?
    - How will you ensure children and adults at risk using the platform know who to contact if they feel uncomfortable, threatened, or would like to report a safeguarding incident or concern?
    - What is your code of conduct for the group? How will you communicate this with everyone involved?
    - Who will be responsible for reviewing the group to ensure appropriate communication and to address and report any issues?
    - In addition to yourself, which members of staff will be included?

- For information on hosting a live online session please see the Trust's virtual event guide.

4.4 Posting on social media

- The Trust requires all staff, who communicate on behalf of the Trust on social media, to always disclose their name and their relationship with the Trust. It is not acceptable to use aliases or otherwise deceive people:

    - Staff must identify themselves (name) and, when relevant, their role, when discussing Trust related matters, this transparency is important for post credibility. Don’t assume people know who you are.
    - When publishing content online that is relevant to the Trust it is important to make it clear you are speaking for yourself and not on behalf of the Trust. Use a disclaimer such as: "The comments are my own and don't necessarily represent HIWWT’s positions, strategies or opinions."
    - See Annex F: Twitter Guidelines for Staff for details of how to write your profile.

- By identifying yourself as working for the Trust, ensure that content associated with you is consistent with your role and does not compromise the Trust’s brand and reputation. Be aware that taking public positions online that are counter to the Trust’s interests might cause conflict.

- Respect privacy and confidentiality – never publish, post, or release confidential information:
    - Be conscientious regarding any personally identifiable information that is used.
    - Do not post anything related to colleagues and business sensitive information about business partners or stakeholders without written permission.
    - Do not give out personal data or disclose non-public information from the Trust, including confidential information, business performance, or other sensitive matters.
    - ***Annex B: Privacy and Confidentiality*** provides details on what not to disclose on social media.

- Respect intellectual property. Do not claim authorship of something that is not yours:
    - Respect copyright, trademarks, fair use, financial disclosure laws, rights of publicity, and other third-party rights on social media, including with regard to user-generated content (UGC).
    - If you post or reference material that is protected by intellectual property rights you must ensure you have taken the right steps to get approval to do so, and that citations are accurate.

- Do not post abusive content, "adult" content, illegal content, offensive content, discriminatory content and racist language, doing so would result in disciplinary action.

See ***Annex C: Posting on Social Media*** for more information about what and how to write on social media.

Complaints and Trolls

- If staff come across negative or disparaging posts about the Trust , its staff or anyone or anything closely associated with the Trust, or see third parties trying to spark negative conversations, they should not react and should instead pass the details of the post(s) on to a member of the Executive team or someone in the Communications Team.

- If you feel that comments or complaints received online are malicious, persistent or unfair, please speak to the Communications Team to discuss the best way to respond.

- Any incident of a scale or nature that poses a potential reputational risk to the Trust should be handled in accordance with the Trust's Serious Issue Procedure.

5. Relevant legislation and statutory guidance

Employees and employers should be aware that their online behaviour could break defamation, data protection or privacy laws e.g. if an employee posts damaging or defamatory comments about an organisation or its products or publishes sensitive data; or if an employer divulges protected personal data, such as giving away details of salary, political or religious beliefs or disciplinary records.

The following legalisations are relevant to this Policy:

- The Human Rights Act 1998
- The Data Protection Act 1988
- The Regulation of Investigatory Powers Act 2000
- Malicious Communications (NI) Order 1988
- Communications Act 2003
- General Data Protection Regulations, 2018

Details can be found in ***Annex D: Relevant legislation and statutory guidance***

6. Training, Governance and Policy Review

The Trust is committed to ensuring that safe processes are in place for all staff whose work brings them into contact with social media. This process includes:

- All existing staff will be provided with training through a presentation at a staff meeting, and any future updates to the policy will be provided at future staff meetings.
- The Trust will ensure that all new staff, and current staff, will see this Policy and all related procedures and guidelines. Staff will be required to sign a declaration to state they have read and understood the policy via IRIS, and by doing so agree to abide by the necessary requirements.
- New staff will receive training at their induction and receive a copy of the Policy
- A quick reference guide will be given to staff and volunteers as an overview of the key areas of the policy.
- Volunteer groups such as Wildlife Watch, who have a more active role on social media, will be sent the training presentation and a copy of the Policy.

Governance
The Director of Fundraising and Marketing is the lead member of staff for the Policy. The Executive Team will have ownership of the Policy and will feed into the annual review, as well as doing a review of incidents and associated actions quarterly. The Policy and all reviews will go to Council for Trustees to approve.

Policy review
The Trust will undertake an annual review of this Policy in light of any incidents and lessons learnt, changes in legislation or new Government guidance. The review will be by carried out by the Executive Team, led by the Director of Fundraising and Marketing.

7. Monitoring and Compliance

Monitoring of social media will be done only when necessary, if there is legitimate interest to ensure the policy is being complied with. Information obtained through monitoring will only be shared with HR, your line manager and other managers linked to the area of work, and only if there are reasonable grounds to believe there has been a breach in the Policy.

Incident reporting

This Policy sets out steps which must be taken should a breach of the Policy occur.

If staff or volunteers are aware of a suspected or confirmed breach of this Policy they must speak to a Designated Social Media Lead immediately (even out of hours or over a weekend).

Any incident should be responded to in accordance with this Policy and, where necessary, the appropriate agencies should be informed as quickly as possible.

Annex E – Procedure for Reporting Incidents details the procedure to be followed for reporting concerns or disclosures, both internally and externally.

Annex A: Forms of cyberbullying

Cyberbullying refers to activity that includes, but is not limited to:

1. Harassment - this involved posting, sharing or sending offensive, malicious, threatening or inappropriate comments, photographs or videos to an individual/group, that are negative, harmful, false, or contain derogatory content about someone else.
Cyberstalking is one form of harassment that involves continual and often threatening messages, and can lead to physical harassment in the offline world.

2. Flaming - similar to harassment, but it refers to an online fight exchanged via emails, instant messaging or chat rooms. It is a type of public bullying that often directs harsh language, or images to a specific person.

3. Exclusion - involves limiting interaction to cliques/groups. It is the act of intentionally singling out and leaving a person out from an online groups such as emails, chats and sites. The group then subsequently leave malicious comments and harass the one they singled out.

4. Outing - when personal and private information, pictures, or videos are shared publicly causing embarrassment or humiliation.

5. Masquerading - when a fake identity is created to harass someone anonymously (or they impersonate someone else to send malicious messages to the victim).

If harassment is related to a particular characteristic of the individual, e.g. race, sex, etc it is prohibited under antidiscrimination legislation and could constitute a criminal offence.

Annex B: Privacy and Confidentiality

Information that must not be disclosed on social media

- **Finances and figures:**

  Non-public financial or operational information. This includes strategies, forecasts and anything that has a financial figure associated with it. If it is not already public information, it is not a member of staff's job to share it publicly.

- **Personal Information:**

  Never share personal information about staff, volunteers or any other stakeholder.

- **Legal Information:**

  Do not share anything to do with a legal issue or legal case without checking with HR.

- **Anything that belongs to someone else:**

  Do not post anything that belongs to someone else e.g. music, copyrighted publications, logos or images that are trademarked. Always give people proper credit for their work.

Annex C: Social Media Code of Conduct

Trust staff must be personally responsible for the content they publish online and be mindful that what is published will be public for a long time.

Exercise Good Judgement

Respect your audience, be careful and considerate at all times. Do not post or add comments including:

- Anything that may harm the good will or reputation of the Trust or any disparaging information about the organisation.
- Any slurs, insults, or otherwise demeaning, inflammatory, critical, argumentative, disparaging, discriminatory or harassing content concerning any supporter, employee or other person associated with the Trust or its competitors.
- Anything that could be considered discriminatory or harassing such as making offensive or derogatory comments relating to sex, gender, race (including nationality), disability, sexual orientation, religion or belief, or age.
- Post images that are discriminatory, offensive or inappropriate or link to such content.

By posting abusive content, "adult" content, illegal content, offensive content, discriminatory content and racist language would result in disciplinary action.

Be Authentic and Accurate

Be yourself, you do not always have to be formal in the way you deliver your content. However, make sure any information you post is accurate and consistent with our role as the local experts in nature and wildlife. Always be truthful and not misleading, it must be possible to prove any claims made online. If you are not sure about something then take advice before answering specific questions.

If you do make a mistake, admit it quickly. For example, if you are posting a blog you can modify your earlier post as long as you make it clear that you've done so.

Political opinion

The Trust supports individuals' rights to engage personally with political parties and activities. However, as a charity, we must be seen to be non-party political. This means that on issues directly or indirectly related to our area of work, such as wildlife and environmental policy or Brexit, we should not post or share any views that may be seen as supporting or criticising one or more political party or that could influence other people's support for political parties.

Response times

People expect answers and responses quickly online. Try to answer questions and respond to questions and questions as soon as you can. Some questions do require a bit of research to answer fully but you should post a holding response within 24 hours.

Annex D: Relevant legislation and statutory guidance

- **The Human Rights Act 1998**

  Article 8 gives a 'right to respect for private and family life, home and correspondence'. Case law suggests that employees have a reasonable expectation of privacy in the workplace.

- **The Regulation of Investigatory Powers Act 2000**

  Covers the extent to which organisations can use covert surveillance.

- **Communications Act 2003**

  This Act confers functions on the Office of Communications; including making provision about the regulation of the provision of electronic communications networks and services. This Act makes it a criminal offence to send or cause to send "...by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character." It also makes it a criminal offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a person sends or causes to send by means of a public electronic communications network, a message that they know to be false, or persistently makes use of a public electronic communications network.

- **General Data Protection Regulation, May 2018**

  The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual.

Annex E: Procedure for Reporting Incidents

Designated Social Media Leads:

Primary:
Catherine Day, Director of Fundraising and Marketing and Communications.
Contact details – direct line 01489 774439, switchboard 01489 774400 or mobile 07825 201651

Secondary:
Elenya Lendon, Digital Communications Officer
Contact details – direct line 01489 774450, switchboard 01489 774400 or mobile 07469 855839

Tertiary:
Hannah Terrey, Director of Advocacy and Engagement
Contact details - direct line 01489 774430, switchboard 01489 774400 or mobile 07825 201612

Out of hours or weekend: contact the Designated Social Media Lead and ensure a clear message is left if no immediate answer.

Procedure:

1. Suspected or confirmed breach of Policy.

2. Ensure that the Designated Social Media Lead is spoken to immediately (even out of hours or over a weekend).

3. Complete a Record of Concern as fully and quickly as possible and send to Designated Social Media Lead who will save securely.

4. Inform Line Manager as soon as possible to ensure that another person is aware that an issue has arisen (but ensure confidentiality is maintained).

5. Designated Social Media Lead review Record of Concern and decides on next step(s) in consultation with reporting person (e.g. If breach includes a child or vulnerable adult inform Children’s or Adult Services and/or the school).

6. If there are no further concerns or no further action required by the Trust – Record of Concern signed off by Designated Social Media Lead and confidential summary of incident reported quarterly to Executive Team and Council.

Annex F: Social Media Guidelines for staff

Why?

- Widen the Trust's sphere of influence by reaching new audiences and developing new relationships.
- Monitor opinion through discussions about topics, people or institutions that are of interest or relevant.
- Communicating with peers and directly engaging in discussion across the conservation and environmental sector.
- Keeping abreast of the latest news and identifying opportunities for the Trust to engage e.g. picking up on and commenting on an issue being discussed by the media

Creating your profile

- **Username and photos**
  - Use your real name and a real photo of yourself for your profile picture e.g. @HannahTerrey @Debbie_Tann @ChristopherLycett
  - Header image – you could be more creative with this, it could represent your area of work e.g. skills or geographical area. This could incorporate the Trust's logo if you are solely using the account for work-related activity.
- **Description**
  - Include key words such as:
    - Your job title
    - Hampshire & Isle of Wight Wildlife Trust
    - Protecting wildlife sites
    - Nature reserve
    - Inspiring young people
  - Include the Trust's website if room allows hiwwt.org.uk
  - Include relevant hashtags e.g. #WilderHampshire #WilderFuture #WilderWight #FishlakeMeadows
  - Include the Trust's main social handle e.g. Twitter @hantsiwwildlife
  - Be accurate and positive in your description.
  - Make it clear that you are speaking for yourself by including a statement such as 'views are my own'.

Here is a good example:

Director of Comms at Hampshire & Isle of Wight Wildlife Trust (@HantsIWWildlife) Twittering on about nature. Working for a #wilderFuture. Views my own.

Posting:

- By identifying yourself as working for the Trust you ensure that content associated with you is consistent with your role in the organisation and doesn't compromise the Trust's brand and reputation.

Always remember that what you are writing can easily be shared and seen by a wider audience than you may anticipate.

- If you are talking about your work, identify yourself clearly e.g. your role - this transparency is important for post credibility. Don't assume people know who you are.

- Be truthful and not misleading – any claims made online should be able to be substantiated.

- Only post meaningful, respectful comments - in other words, no spam and no remarks that are off-topic or offensive.

Use of hashtags and mentioning users

- Think of a hashtag as a search term people might use to find similar content or follow a particular issue.

- Using excessive hashtags will annoy followers and can confuse the message; one or two is normally plenty.

Which hashtags to use

- Regular hashtag used by HIWWT to represent our work:

  #LoveWildlife
  #WilderHampshire
  #WilderWight
  #MyWildlife
  #WilderFuture

- Personal to your area of work, you might want to highlight a nature reserve, a species or a project :

  #BlashfordLakes
  #FishlakeMeadows
  #YoungNaturalists
  #SecretsoftheSolent

  #Watervole

- You might be linking to an important discussion area already on Twitter

  #EnvironmentBill
  #NetGain

It is a good idea to include someone else's Twitter handle if what you're saying is relevant to a partners or similar etc e.g. @Vinehousefarm

When linking to another account you can either put it within your tweet, or to save characters you can tag them when uploading an image.

It is not just about posting; you should also be following and monitoring

Follow relevant users i.e. other charities, celebrities, colleagues, local influences (e.g. media, MPs etc).

Interacting with your followers is a great way of encouraging engagement:

1. Reply to people as often as possible
2. Share others' posts (if the subject matter is aligned with our views)

3. Quoting posts to add the Trust's opinion
4. Favourite posts to show followers that you're seeing their content

Further help and guidance

Tone of voice

It's a fine balancing act! Try to be friendly and approachable, whilst still appearing as an authority. Using too much jargon can 'turn off' potential audiences, however there are many conservation professionals online so it's also important to ensure they feel that you're knowledgeable on your subject area.

Irregular activity

When something big is happening in your area of work people will expect you to be doing some extra social activity, however even when there is nothing specific happening people will still expect a regular stream of activity and engagement. Do not leave long gaps where you become absent. As a minimum, monitor feeds to participate in relevant conversations and share others' useful content.

Responses times

People expect answers and responses quickly. Try to answer questions and respond to questions as soon as you can. Some questions do require a bit of research to answer fully but you should post a holding response within 24 hours.