

Technology and Social Media Policy



Operational Owner	Education Manager: Helen Ward
Trustee Owner	Lindsey Slater
Effective date:	24/09/22
Review date:	24/09/24
Related documents	Equality and Diversity policy Safeguarding Policy Data protection policy

Approval History

Version	Reviewed by	Amendment History	Approved by	Date
1.0	Emma Hughes/Jane Sullivan	New Policy	Management Committee	30/3/21
1.1	Emma Hughes	Updated with staffing changes	Chair of Trustees	24/09/22

Scope

The policy is separated into guidance for use of accounts and devices owned by Susan's Farm and guidance for use of privately owned accounts devices where use may affect the functioning and reputation of Susan's Farm.

The policy applies to staff (including volunteers) and beneficiaries and states clearly where there are different responsibilities.

By "social media", we refer to a variety of online communities like blogs, social networks, chat rooms and forums.

The policy's purpose is to:

- Provide practical advice to avoid issues that might arise regarding the use of digital technology and social media
- Ensure compliance with relevant statutes/guideline e.g. GDPR, Safeguarding
- Protect the reputation of Susan's Farm
- Ensure the security of devices, data and accounts
- Set out guidance for 'fair use' of Susan's Farm's devices
- Support beneficiaries in safe use of social media with reference to the Safeguarding Policy
- Protect staff from work matters intruding in their time outside of work.

Devices owned by Susan's Farm

All of Susan's Farm's devices are protected with a PIN/pattern/password which should be changed regularly every three months.

Susan's Farm's devices should not be used for personal use other than on an exceptional basis. They should never be used for accessing inappropriate content.

Particular care should be taken not to use Susan's Farm's devices for activities which could lead to a security risk e.g. online quizzes or voucher deals

Software should be updated regularly. Minor updates are usually done automatically. We will review software for major updates every 1-2 years and will seek technical support from a qualified professional where required.

Photographs or videos of people should only be should only be taken and stored in accordance with our Privacy policy.

Accounts owned by Susan's Farm

All social media accounts should be monitored for evidence of hacking and to remove false/damaging content as soon as possible. Staff should also be aware that fake accounts can cause reputational damage and should report anything suspicious as soon as possible to the General Manager.

Privacy settings should be reviewed every six months and access removed as soon as a member of staff leaves.

Staff with responsibility for posting content to Susan's Farm accounts are expected to use the Business Manager App for their own privacy and to allow control of notifications outside of work hours.

Susan's Farm social media is a place where we can exchange information, promote our educational and charitable work, share nature and experiences of the farm and have fun. When posting content/comments staff should remain productive and avoid damaging the charity in any way. Specifically:

- Be respectful, polite and patient when engaging in conversations on the charity's behalf. You should be especially careful when making declarations or promises towards customers and stakeholders.
- Avoid speaking on matters outside your field of expertise when possible. Everyone should be careful not to answer questions that fall under somebody else's responsibility.
- Follow our data protection policy specifically never using a photo of a person without their written consent to use their data for this purpose
- Avoid deleting or ignoring comments for no reason. We should listen and reply to criticism.

- Never post discriminatory, offensive or libellous content and commentary.

Specific staff members/trustees will be given authority to post on Susan's Farm social media accounts as required to fulfil their duties.

Personal Devices

Staff and volunteer's personal devices should not be used for work purposes where personal information is involved (e.g. photos of people, telephone numbers) in order to ensure compliance with our data protection policy.

School groups will adhere to their school's policy on personal devices during visits.

Alternative Provision beneficiaries are required to leave their mobile phones in their secure locker during their session, however appropriate use of personal devices will be identified and managed in accordance with the individual's personal learning plan/positive behaviour agreement.

Staff and volunteers should be alert to beneficiaries use of their personal devices in case of concerns about their online safety and refer to the safeguarding policy.

Personal Accounts

Staff may access their personal accounts at work, however they are expected to act responsibly and ensure productivity isn't affected.

Staff are expected to be careful when posting on social media. They are expected to adhere to the confidentiality policies at all times. With reference to the charities Equality, Diversity and Inclusion policy, staff should also be cautious about posting any content that may make working with colleagues and beneficiaries more difficult.

We advise staff to:

- Ensure others know that your personal account or statements do not represent the Farm. You should not state or imply that your personal opinions and content are authorised or endorsed by the Farm. We advise using a disclaimer such as “opinions are my own” to avoid misunderstandings.
- Avoid any defamatory, offensive or derogatory content. It may be considered as a violation of our company’s Equality, Diversity and Inclusion policy, if directed towards colleagues, beneficiaries or other stakeholders.

Training

It is a statutory requirement that schools provide safeguarding training to their staff once a year **as a minimum**. The importance of current online safety issues being addressed within such training is more important than ever. At Susan’s Farm we will also ensure that our training includes e-safety as part of our Safeguarding approach.

The OSA Certificate of Online Safety has been developed to help address this requirement. Free to access for all staff in UK schools, the Certificate also provides tangible data that proves to governors and inspectors that staff have understood such training.

As part of our annual training plan, this training is a requirement for all staff, trustees, and independent volunteers.

[Click here to get started.](#)

[Click here to download the user guide.](#)