Online safety policy

Sweet Futures Limited

Author:	Geoff Littlewood	
Approved by:	Claire Scott	**Date:** 29/10/2019
Last reviewed on:	29/10/2019	
Next review due by:	29/10/2020	

Contents

---

1. Aims

Our company aims to:

- Have robust processes in place to ensure the online safety of young people, staff, and volunteers
- Deliver an effective approach to online safety, which empowers us to protect and educate our staff, and young people in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy reflects existing legislation, including but not limited to the Equality Act 2010.

This policy complies with our articles of association.

3. Roles and responsibilities

3.1 The company board

The company board has overall responsibility for monitoring this policy.

All staff will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the company's IT systems and the internet (appendix 3)

3.2 The CEO

The CEO is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the company.

3.3 The designated safeguarding lead

Details of the company's DSL and deputy are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in the business, in particular:

- Supporting the CEO in ensuring that staff understand this policy and that it is being implemented consistently throughout the company
- Working with the CEO and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the company behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

3.4 IT Management

The CEO is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep young people safe from potentially harmful and inappropriate content and contact online while at our premises, including terrorist and extremist material
- Ensuring that the company's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the company's IT systems on a quarterly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the company behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the company's IT systems and the internet (appendix 3), and ensuring that young people follow the company's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the CEO of any concerns or queries regarding this policy
- Ensure their young person has read, understood and agreed to the terms on acceptable use of the company's IT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the company's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating young people about online safety

Young people will be taught about online safety as part of the training program, if applicable:

Young people in **Key Stage 4 and 5** will be encouraged:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered where relevant.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

5.2 Preventing and addressing cyber-bullying

Staff are encouraged to find opportunities to use aspects of the training program to discuss cyber-bullying.

In relation to a specific incident of cyber-bullying, the company will follow the processes set out in the company behaviour policy. Where illegal, inappropriate or harmful material has been spread among young people, the company will use all reasonable endeavours to ensure the incident is contained and reported to the visiting school/college or parent/carer, where applicable.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6. Acceptable use of the internet in the company

All young people, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the company's IT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the company's terms on acceptable use if relevant.

Use of the company's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

7. Young people using mobile devices in company premises

Young people may bring mobile devices into the company premises but are not permitted to use them during working hours.

Any use of mobile devices in the company's premises by young people must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a young person may trigger disciplinary action in line with the company behaviour policy.

8. Staff using work devices outside working hours

Staff members using a work device outside working hours must not install any unauthorised software on the device and must not use the device in any way which would violate the company's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside the workplace.

If staff have any concerns over the security of their device, they must seek advice from the CEO.

Work devices must be used solely for work activities.

9. How the company will respond to issues of misuse

Where a young person misuses the company's IT systems or internet, we will:

Revoke access immediately to the IT systems from the young person

Discuss the issue with the individual and, where applicable, supporting staff from the visiting school/college

Notify either the DSL from the visiting school/college, or the parent/carer in cases where the young person is using the services directly.

Where a staff member misuses the company's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The company will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every 2 years by the CEO. At every review, the policy will be shared with the company board.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT and internet acceptable use policy

Appendix 1: KS4 and KS5 acceptable use agreement (young people and parents/carers)

ACCEPTABLE USE OF THE COMPANY'S IT SYSTEMS AND INTERNET: AGREEMENT FOR YOUNG PEOPLE AND PARENTS/CARERS	
Name of young person:	
I will read and follow the rules in the acceptable use agreement policy **When I am using the internet at The Shop I will:** • Always use The Shop's IT systems and the internet responsibly and for educational purposes only • Only use them when a tutor is present, or with a tutor's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my tutor or parent/carer • Tell a tutor (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my tutor has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a tutor • Use any inappropriate language when communicating online, including in emails • Log in to the shop's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into The Shop:** • I will not use it during working hours without a tutor's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that The Shop will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (young person):	**Date:**
Parent/carer's agreement: I agree that my young person can use the company's IT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for young people using the company's IT systems and internet, and for using personal electronic devices in The Shop, and will make sure my young person understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, young people, volunteers and visitors)

ACCEPTABLE USE OF THE COMPANY IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFFYOUNG PEOPLE,VOLUNTEERS AND VISITORS	
Name of staff member/young person/volunteer/visitor:	
When using the company's IT systems and accessing the internet in The Shop, or outside The Shop on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the company's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the company's network • Share my password with others or log in to the company's network using someone else's details • Take photographs of young people without checking with tutors first • Share confidential information about the company, its young people or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to The Shop	
I will only use the company's IT systems and access the internet in The Shop, or outside The Shop on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the company will monitor the websites I visit and my use of the company's IT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside The Shop, and keep all data securely stored in accordance with this policy and the company's data protection policy. I will let the designated safeguarding lead (DSL) and CEO know if a young person informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the company's IT systems and internet responsibly, and ensure that young people in my care do so too.	
Signed (staff member/young person/volunteer/visitor):	**Date:**

Appendix 3: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**