IT and internet acceptable use 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. Introduction and aims 2
2. Relevant legislation and guidance 2
3. Definitions 3
4. Unacceptable use 3
5. Staff (including volunteers and contractors) 4
7. Parents/Carers 6
8. Data security 7
9. Internet access 8
10. Monitoring and review 8
11. Related policies 8
Appendix 1: Facebook cheat sheet for staff 9
Appendix 2: Acceptable use of the internet: agreement for parents and carers 11
Appendix 3: Acceptable use agreement for young people 12
Appendix 4: Acceptable use agreement for younger people 13
Appendix 5: Acceptable use agreement for staff, volunteers and visitors 14

---

1. Introduction and aims

IT is an integral part of the way our company works, and is a critical resource for young people, staff, volunteers and visitors.

However, the IT resources and facilities our company uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of company IT resources for staff, young people and parents/carers
- Establish clear expectations for the way all members of the company and community engage with each other online
- Support the company's policy on data protection, online safety and safeguarding
- Prevent disruption to the company through the misuse, or attempted misuse, of IT systems

This policy covers all users of our IT facilities

Breaches of this policy may be dealt with under our behaviour and staff code of conduct policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000

- Keeping Young personren Safe in Education 2018

3. Definitions

- **“IT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service
- **“Users”:** anyone authorised by the company to use the IT facilities
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the company to perform systems administration and/or monitoring of the IT facilities
- **“Materials”:** files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the company’s IT facilities by any member of the organisation. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the company’s IT facilities includes:

- Using the IT facilities to breach intellectual property rights or copyright
- Using the IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the company’s policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the company, or risks bringing the company into disrepute
- Sharing confidential information about the company, its staff, or other members of the organisation
- Connecting any device to the IT network without approval from authorised personnel
- Setting up any software, applications or web services on the company’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data
- Gaining, or attempting to gain, access to restrITed areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the IT facilities
- Causing intentional damage to IT facilities
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the company

- Using websites or mechanisms to bypass the company's filtering mechanisms

This is not an exhaustive list. The company reserves the right to amend this list at any time. The CEO will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the company's IT facilities.

4.1 Exceptions from unacceptable use

Where the use of company IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the CEO's discretion.

4.2 Sanctions

Young people and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the company's policies on behaviour/staff discipline/staff code of conduct/etc..

5. Staff (including volunteers and contractors)

5.1 Access to company IT facilities and materials

The company's CEO manages access to the company's IT facilities and materials for company staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the company's IT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the CEO

5.1.1 Use of phones and email

The company provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the company has provided.

Staff must not share their personal email addresses with parents/carers and young people, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the CEO immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents/carers or young people. Staff must use phones provided by the company to conduct all work-related business.

Company phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use company IT facilities for personal use subject to certain conditions set out below. Personal use of IT facilities must not be overused or abused. The CEO may withdraw permission for it at any time or restrict IT access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during working hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no young people are present
- Does not interfere with their jobs, or prevent other staff or young people from using the facilities for work or educational purposes

Staff may not use the company's IT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the company's IT facilities for personal use may put personal communications within the scope of the company's IT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the company's personal device policy.

Staff should be aware that personal use of IT (even when not using company IT facilities) can impact on their employment by, for instance putting personal details in the public domain, where young people and parents/carers could see them.

Staff should take care to follow the company's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The company has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.4 Company social media accounts

The company has an official social media pages (Facebook/Twitter), managed by CEO. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The company has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of company network and use of IT facilities

The company reserves the right to monitor the use of its IT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited

- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised IT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The company monitors IT use in order to:

- Obtain information related to company business
- Investigate compliance with company policies, procedures and standards
- Ensure effective company and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6.3 Unacceptable use of IT and the internet outside of company

The company will sanction young people, in line with the [behaviour/discipline policy], if a young person engages in any of the following **at any time** (even if they are not on company premises):

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the company's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the company, or risks bringing the company into disrepute
- Sharing confidential information about the company, other young people, or other members of the organisation
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the company's IT facilities
- Causing intentional damage to IT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/Carers

7.1 Access to IT facilities and materials

Parents/Carers do not have access to the company's IT facilities as a matter of course.

However, parents/carers working for, or with, the company in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the company's facilities at the CEO's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the company online

We believe it is important to model for young people, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their young person, especially when communicating with the company through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

8. Data security

The company takes steps to protect the security of its computing resources, data and user accounts. However, the company cannot guarantee security. Staff, young people, parents/carers and others who use the company's IT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the company's IT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or young people who disclose account or password information may face disciplinary action. Parents/Carers or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the company's IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the company's IT facilities.

Any personal devices using the company's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the company's data protection policy.

8.4 Access to facilities and materials

All users of the company's IT facilities will have clearly defined access rights to company systems, files and devices.

These access rights are managed by CEO.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the CEO immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The company ensures that its devices and systems have an appropriate level of encryption.

Company staff may only use personal devices (including computers and USB drives) to access company data, work remotely, or take personal data (such as young person's information) out of company if they have been specifically authorised to do so by the CEO.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the CEO.

9. Internet access

The company wireless internet connection is secured.

Access to the wireless internet connection should be requested via the CEO. No other user should disclose any passwords.

10. Monitoring and review

The CEO monitors the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the company.

This policy will be reviewed every 2 years.

11. Related policies

This policy should be read alongside the company's policies on:

- Online safety
- Safeguarding and young person protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: Facebook cheat sheet for staff

If you have a social media policy, adapt this in line with that policy. You may decide to hand this cheat sheet out to your staff as a standalone document and remove it from here. If so, renumber the following appendices and check for references to appendix 1 in the policy.

Don't accept friend requests from young people on social media

10 rules for company staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile pITure to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your young people
6. Don't use social media sites during company hours
7. Don't make comments about your job, your colleagues, our company or your young people online – once it's out there, it's out there
8. Don't associate yourself with the company on your profile (e.g. by setting it as your workplace, or by 'checking in' at a company event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents/carers or young people)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, young people and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile pITure, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A young person adds you on social media

- In the first instance, ignore and delete the request. Block the young person from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile pITure
- If the young person asks you about the friend request in person, tell them that you're not allowed to accept friend requests from young people and that if they persist, you'll have to notify management team and/or their parents/carers. If the young person persists, take a screenshot of their request and any accompanying messages
- Notify the management team or the CEO about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's/carer's friend request or message might set an unwelcome precedent for both you and other tutors at the company
    - Young people may then have indirect access through their parent's/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current service user or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or the management team should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of young person:**	
Online channels are an important way for parents/carers to communicate with, or about, our company. The company uses the following channels: • Our official Facebook page • Email/text groups for parents/carers (for company announcements and information) • Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their young person's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the company via official communication channels, or using private/independent channels to talk about the company, I will: • Be respectful towards members of staff, and the company, at all times • Be respectful of other parents/carers and young personren • Direct any complaints or concerns through the company's official channels, so they can be dealt with in line with the company's complaints procedure I will not: • Use private groups, the company's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the company can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the company's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other young people. I will contact the company and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any young person other than my own, unless I have the permission of other young person's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for young people

Acceptable use of the company's IT facilities and internet: agreement for young people and parents/carers	
Name of young person:	
When using the company's IT facilities and accessing the internet in company, I will not: • Use them for a non-educational purpose • Use them without a tutor being present, or without a tutor's permission • Use them to break company rules • Access any inappropriate websites • Access social networking sites (unless my tutor has expressly allowed this as part of a learning activity) • Use chat rooms • 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 • Share my password with others or log in to the company's network using someone else's details • Bully other people I understand that the company will monitor the websites I visit and my use of the company's IT facilities and systems. I will immediately let a tutor or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the company's IT systems and internet responsibly. I understand that the company can discipline me if I do certain unacceptable things online, even if I'm not in company when I do them.	
Signed (young person):	**Date:**
Parent/carer agreement: I agree that my young person can use the company's IT systems and internet when appropriately supervised by a member of company staff. I agree to the conditions set out above for young persons using the company's IT systems and internet, and for using personal electronic devices in company, and will make sure my young person understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger people

Acceptable use of the company's IT facilities and internet: agreement for young people and parents/carers	
Name of young person:	
When I use the company's IT facilities (like computers and equipment) and get on the internet in company, I will not: • Use them without asking a tutor first, or without a tutor in the room with me • Use them to break company rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my tutor said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a tutor first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the company will check the websites I visit and how I use the company's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a tutor or a member of staff I know immediately if I find anything on a company computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the company's IT systems and internet. I understand that the company can discipline me if I do certain unacceptable things online, even if I'm not in company when I do them.	
Signed (young person):	**Date:**
Parent/carer agreement: I agree that my young person can use the company's IT systems and internet when appropriately supervised by a member of company staff. I agree to the conditions set out above for young persons using the company's IT systems and internet, and for using personal electronic devices in company, and will make sure my young person understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, volunteers and visitors

Acceptable use of the company's IT facilities and the internet: agreement for staff, volunteers and visitors	
Name of staff member/volunteer/visitor:	
When using the company's IT facilities and accessing the internet in company, or outside company on a work device, 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 • Share confidential information about the company, its young persons 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 company	
I understand 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 company, 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 IT manager 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/volunteer/visitor):	**Date:**