SENTALK

Sen Talk CIC's IT and Acceptable Use policy

This policy applies to all staff, including the management committee, trustees, paid staff, volunteers, service users and anybody working on behalf of Sen Talk CIC.

Purpose

An IT acceptable use policy (AUP) describes the rights and responsibilities of anyone using resources, such as computers, the Internet, social media, video cameras and so on. It explains the procedures they are expected to follow and makes clear what is considered acceptable behaviour when using it, helping to ensure user safety and organisational security and maintain good practice where possible.

Who is covered by the policy?

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual, agency staff, volunteers and any service users accessing Sen Talk. This is to ensure that;

- We are able to offer effective and efficient IT facilities within available resources
- We can generate savings by having a co-ordinated approach to our purchasing hardware and software
- On-costs and on-going IT support and maintenance can be planned effectively
- Access to IT is appropriate to the requirements of any given role
- Internal training can be carried out effectively
- Systems are compatible throughout the organisation where possible
- The safety and well being of all staff, volunteers and service users are paramount

Responsibility for implementation of the policy

The Director has overall responsibility for the effective operation of this policy. This policy will be under scrutiny of the board of trustees.

All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Chief Executive Office.

Purchasing equipment, software and services

Within budgetary constraints we aim to ensure that access to IT facilities is fair and equitable whilst being appropriate for the job to be carried out. Some projects will have specific funding for computer equipment; other staff will have access to shared computers.

Any purchase or acquisition of all computers, software and services should be agreed in advance and authorised by the appropriate Project Manager and authorised by the Director.

Hardware

Please treat all hardware with care and respect. Equipment that has broken or expired should be repaired where possible, otherwise disposed of responsibly. Speak to the Project Lead and/or the Director when instances occur. It is the employee's responsibility to take care of equipment that has been allocated, and failure to do so could result in the cost of replacement falling on individuals.

Software

- Sen Talk use Microsoft Office 365 cloud software, which includes share point and the internal database system Lamplight. The software will be automatically updated on a regular basis.
- All programmes loaded onto computers must be licensed for use within the organisation. Software not licensed for use at Sen Talk should not be loaded onto any Sen Talk computer or equipment. The consequences for Sen Talk, discovered using unlicensed material, could be severe and result in hefty fines.
- A record of all software installed, licenses and applications will be kept centrally.

- Do not download software, software updates or introduce new software to work on your PC or laptop without first checking with the Project Lead and or the Director. Virus software is maintained and periodically updated. If your PC does acquire a virus, please follow the de-bugging instructions from the anti-virus software and report the incident to the Project Manager.

Faults

Faults should be reported to your Project Manager immediately. They should try to address the issue themselves. If they are not able to your Project should seek advice from the Director which may require assistance from our outsourced IT Support company, Littleshock.

Security and Safety

Staff are responsible for ensuring that computer hardware is secure and should speak to the Project Manager and or the Director about secure storage and if they have any concerns about possible theft. This is particularly true of laptops which can be easily taken. No confidential client or staff data should be kept on a laptop that is being used off site.

You must take the appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data e.g. password protection for all PCs; and log off a PC if leaving the room (i.e. press the windows key + L = this locks a computer). This coincides with company GDPR and Data Protection Policy. You must not allow third parties to access any equipment

Safeguarding and use of equipment

We pay particular attention to systems that are used by children and young people. Additional security measures should be in place to block access to inappropriate sites and materials, agreed by the Project Manager and Director. Children and young people are not authorised to use any of the communal computers in the building. Service users must be supervised when using company resources to ensure that the use is proper, safe and secure.

All equipment will be checked regularly for safety in line with Sen Talks' regular portable appliance testing schedule. These checks will be completed every 12 months to ensure that equipment in safe and secure for use.

Obviously, it is advisable to avoid eating or drinking around PCs and similar equipment to avoid accidents and damage to the machines. When using IT equipment with users and clients it is best to adopt a ‘no food or drink in the room’ approach.

Email and email attachments

Only use email for work related purposes. Sending an email is sometimes far easier than speaking to someone face to face or even talking on the telephone, especially if you have something difficult to say. Once an email has been sent it cannot be retrieved. Think before you hit the send button! Do not email in anger or annoyance – avoid sending aggressive or abusive emails.

Please do not pass on chain mail, jokes, spam or hoax virus warnings etc.

Sending group emails

Care should be taken when attaching documents to ensure there is no infringement of copyright and you must not disclose confidential information. If the attachment is large, then please consider forwarding a link to a file uploaded or sending a compressed zip file. When emailing more than one recipient, please blind copy (BCC) so you are not sharing confidential information without permission.

Absolute vigilance should be taken when emailing, if you are unsure about the origin of an email attachment or message, please do not open it before you contact the Project Manager and Director. Also please make contact if you are receiving large amounts of ‘junk mail’.

Internet use

The internet should be used in the main for work purposes only. However, we understand that you may wish to use the internet during a work break for your own purposes and provided that your manager agrees, and you follow the guidelines contained within this policy that is fine.

Social media websites

This policy outlines the standards Sen Talk CIC requires staff to observe when using social media, the circumstances in which Sen Talk CIC will monitor your use of social media and the action that will be taken in respect of breaches of this policy. The principles of this policy apply to use of social media regardless of the method used to access it - it covers static and mobile IT/computer equipment, as well as work and/or personal smartphones etc.

Questions regarding the content or application of this policy should be directed to the Chief Executive Officer.

Using work-related social media

Only the Chief Executive Officer is permitted to post material on a social media website in the company’s name and behalf, unless a task has been allocated directly by the Chief Executive Officer to an individual. Anyone who breaches this restriction will face the company's disciplinary procedure.

Approved social media websites for Sen Talk CIC are Facebook, Twitter and Linked In. This list may be updated by Chief Executive Officer.

Before using work-related social media, you must:

- have read and understood this policy and the code of conduct and
- have sought and gained prior written or verbal approval to do so from the Chief Executive Officer.

The roles and functions which will be needed moving forward have been identified as follows:

- tweeting news
- advertising promotions on Facebook
- Sharing of approved images

Personal use of social media

Personal use of social media in the workplace is permitted, subject to certain conditions, as detailed below. It must not be abused or over-used and the company reserves the right to withdraw permission at any time.

The following conditions must be met for personal use to continue:

- use must be minimal and take place substantially outside of normal working hours, for example, breaks and lunchtime
- use must not interfere with business or office commitments

- use must comply with our policies including relevant policies such as Equal Opportunities Policy, Anti-Harassment Policy, Data Protection Policy and Disciplinary Procedure

You are also personally responsible for what you communicate on social media sites outside the workplace, for example at home, in your own time, using your own equipment. You must always be mindful of your contributions and what you disclose about the company. For further details, see Point 7, 'General rules for social media use' below.

General rules for social media use

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules. The same rules would also apply when using social media outside of work:

- Do not post or forward a link to any abusive, discriminatory, harassing, derogatory, defamatory or inappropriate content.
- A member of staff who feels that they have been harassed or bullied, or are offended by material posted by a colleague onto a social media website should inform line manager or Chief Executive Officer
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with line manager and refer to the Sen Talk CIC code of conduct.
- Do not post material in breach of copyright or other intellectual property rights.
- Be honest and open but be mindful of the impact your contribution might make to people's perceptions of the company.
- You are personally responsible for content you publish – be aware that it will be public for many years.
- When using social media for personal use, use a disclaimer, for example: 'The views expressed are my own and don't reflect the views of my employer'. Be aware though that even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.
- You should avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

- Do not post anything that your colleagues or our customers, clients, business partners, suppliers or vendors would find offensive, insulting, obscene and/or discriminatory.
- Do not under any circumstances engage with service users on your personal social media platforms. If a service user has requested to connect, please seek advice from your line manager or the Chief Executive Officer.
- Do not post images of yourself wearing your uniform that may put hinder Sen Talk's reputation or cause offence.
- If you have disclosed your affiliation as an employee of our organisation you must ensure that your profile and any content you post are consistent with the professional image you present to client and colleagues.

Monitoring

Staff email and internet access are not monitored on a regular on-going basis, but we do undertake spot checks to ensure that inappropriate or offensive material is not being accessed or shared within our systems. Any evidence of such access will be fully investigated, and confirmation of such use is likely to lead to disciplinary action. The Director (Annaliese Boucher) will undertake to investigate fully any allegation of accessing or holding inappropriate materials on work computers or portable drives and devices.

The company reserves the right to restrict or prevent access to certain social media websites if personal use is excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the company.

If you notice any use of social media by other members of staff in breach of this policy, please report it to the Project Manager or Director.

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal.

Regular checks are undertaken to ensure that all procedures are being complied with. Staff should also note that their own personal data, files and email accounts should not at any time be held on work PC's or laptops.

Please note – Sen Talk reserves the right to check all material held on work PCs and laptops for operational and security reasons.

Breach of Policy

The penalty applied will depend on factors such as the seriousness of the breach; the nature of the posting; the impact it has had on the organisation or the individual concerned; whether the comments cause problems given the employee's role; whether the employer can be identified by the postings; other mitigating factors such as the employee's disciplinary record etc. Remember the same test of reasonableness applies when dismissing for improper use of social media as it would for any other misconduct dismissal.

Policy review and update

The Director has overall responsibility for the review and update of this policy at the beginning of each year or more regularly as required.

Agreement

All company employees, contractors or temporary staff are required to sign this agreement confirming their understanding and acceptance of this policy.