REGISTERED NUMBER CIC 11373253
All Welcome! All Supported! All Together!

IT & Social Media for Employees Policy and Procedures

Title of Policy: IT and Social Media Policy for Employees
Effective Date: May 2020
Review Date: May 2021
Policy Number: 1
Policy Authorised by: Nicola Williams

Introduction

Allsorts Support Services CIC (which will be referred to as the organisation throughout this policy).

This policy document should be considered in conjunction with all other relevant duties, policies and guidance.

Aim of the Policy

The integrity of our computer system is central to our success as an organisation. This policy aims to ensure that all staff have clear instructions and understand the rules governing the use of our information technology, the internet, email accounts and social media.

Computer Security

All users will be issued with a unique password which will be changed at regular intervals. Access to the system using another employee's password without prior authorisation is likely to result in disciplinary action, including summary dismissal. Computers must be locked when leaving a workstation to stop any unauthorised access.

Users must ensure that critical information is not stored solely within the system. Any critical information should be stored separately on the system. Daily electronic back-ups are carried out on all essential data. If necessary, documents must be password protected.

Care must be taken with any suspicious emails and these must not be opened.

Physical security of IT equipment is to be practised at all times. Portable items should be locked away when not in use and other equipment should be located away from view where possible.

The safekeeping of CDs, DVDs and memory sticks sent from external sources is the responsibility of the person to whom they were sent. All such CDs, DVDs and memory sticks must be checked for viruses by authorised personnel before use. CDs, DVDs and memory sticks generated internally must be kept in a secure place.

Only authorised personnel have the authority to load program software onto a works computer. Any re-configuring or disabling without prior permission is strictly prohibited. Data compatible

with the Company's system may be loaded only after being checked for viruses by authorised personnel. Any employee found to be contravening this may face disciplinary action under the Company's disciplinary procedure.

Computer Software

The Company licences the use of computer software from a variety of outside companies. All our software must be formally authorised by our Manager. No external software may be used without authorisation by the Manager. The Company does not own this software or its related documentation and, unless authorised by the software developer, neither the Company nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Any employee found to be contravening this may face disciplinary action under the company's disciplinary procedure.

Computer misuse

If you have authorised access to a computer in the workplace, this is for the use in connection with the Company's business only. Employees who are discovered unreasonably using the Company's computers for personal and private purposes or vandalising the Company's system will be dealt with under the disciplinary procedure.

Email and the Internet

Email is a fast and reliable means of business communication, so using email accounts set up by the company is encouraged. However, it should be recognised that no system is secure and that at any time emails may find themselves in the public domain. Therefore, anyone sending emails during hours of business must ensure the following:

- Emails must be succinct, clear and good English.
- Authors should not add copy addresses unnecessarily.
- Emails must not be of a nature that may be seen to criticise another employee or demeaning in any way. If there is an issue, constructive guidance should be carried out in a face to face meeting at the earliest opportunity.
- When using group email addresses, such as staff email, authors must place these in the “Bcc...” box rather than the “To...” box in order to prevent the individual email addresses of all the staff in the company being revealed to any third parties to whom the email may later be forwarded.

Allsorts Support Services registered number, contact details must be at the bottom of each email.

The email contact lists are the property of Allsorts Support Services even if they were created by an employee. Employees may not copy or remove any contact list in its entirety for use outside of the Organisation without express permission from the Manager.

Employees are prohibited from sharing any non-business material. No “excessive” time chatting by e-mail for personal and private purposes will be allowed. In addition, offensive remarks, pictures or videos, jokes sent by e-mail, via social networking websites or blogs which are capable of amounting to harassment on the grounds of sex, marital status, race, disability, age, sexual orientation and religion or belief under the terms of the Organisation's policies will be dealt with accordingly.

Nobody is permitted to surf the internet for personal or private use, log on to social networking and video sharing websites such as Facebook, MySpace, YouTube etc or use the Organisation's IT systems to keep a personal weblog during work time unless it is related to the Organisation.

When logging on to and using social networking and video sharing websites and blogs at any time, employees must NOT, without prior permission from the Manager:

- Publicly identify yourself as working for the Organisation, make reference to the Company unless for promotional purposes.
- Conduct yourself in a way that is detrimental to the Organisation that brings the Organisation into disrepute.
- Use your work email address when registering on such sites.
- Include personal information about the Organisation's employees, suppliers, service users without their express consent.
- Make any derogatory, offensive or defamatory comments about the Organisation, it's employees or service users.

Employees must not:

- Make unauthorised orders for personal goods or services by e-mail or internet at work.
- Log on to sexually explicit websites or download and/or circulate pornography or other grossly offensive, obscene or illegal material. This will constitute Gross Misconduct and

render the employee liable to dismissal.

- Disclose any confidential information belonging to the Organisation or its suppliers, service users, partners or any information which could be used by a competitor.

Anybody who is discovered contravening these rules may face serious disciplinary action, including potential Gross Misconduct under the disciplinary procedure.

The Organisation reserves the right to deny, remove or limit e-mail and/or internet access to or from any employee, at any time.

The Organisation also reserves the right to monitor employee's emails and use of the internet at any time.

Social Media – for employees authorised to use Social Media Tools for work purposes

Social media now encompasses a wide range of online activities from social networks such as Facebook and MySpace, professional networks such as Linkedin and personal and company blogs and Twitter (to name a few). There will be many more and this policy will be updated regularly where necessary.

This Organisation recognises that social media will be an important element of driving our business forward. We are also aware that social media will not be used exclusively for business. The following guidelines are intended to help determine acceptable standards when you are online on the Organisation's behalf. However, it should be remembered that personal use that brings the Organisation, its employees or its service users into disrepute will always be totally unacceptable.

You are responsible for what you post; never use the Organisation's name to promote your own ideas. Employees who are permitted to use social media should always remember they are representing the business and reputation; when you are online and interacting with other people on the internet you are speaking on behalf of the Organisation.

Identify yourself as an employee for Allsorts Support Services, we want anyone who interacts on social media activities to represent the best interests and standards of our Organisation. When creating a blog you must gain permission from the Managing Director. Never use a service users name or photos unless we have written permission to do so. Be careful about information you share about yourself and or others within the Organisation, so that your colleagues are treated with respect and their confidentiality.

Do not become involved in arguments or disagreements with conversations or postings relating to the Organisation, if you discover or are approached with a negative complaint, constructive feedback or anything else, you must take it straight to the Manager to deal with.