IT & INTERNET POLICY

VERSION: 3.5

Version	By Author	Reason	Reviewed / Modified	Date Ratified
3.3	HB/TS	Add legislation/further info section	January 2017	April 2017
3.4	HB/TS	Update legal and GDPR sources	January 2018	March 2018
3.5	TS/HB	• New Disposal of Removable Storage Media Section. • Add Linked Policy Section.	January 2019	March 2019
3.5	TS/HB	Review – no change	February 2020	March 2020

This policy applies to all members of the Make Some Noise team including Trustees, staff, volunteers, freelance workers.

Introduction

The Internet and e-mail are essential tools for the Make Some Noise team. However, the use of these tools can expose the organisation to technical, commercial and legal risks if they are not used sensibly.

It should be noted that at this time Make Some Noise utilises the IT and Internet systems controlled and managed by Staffordshire County Council and, as such, this IT and Internet Protection Policy is produced in line with the current County Council ICT Security Policies. Make Some Noise's Safeguarding Policy is interconnected with this IT and Internet Policy.

The aim of this policy document is to:

- Provide guidance on use of the Internet and e-mail at work to minimise the organisation's exposure to these risks
- Explain what Make Some Noise team can and can't do
- Provide some explanation of the legal risks that the team need to be aware of in their use of the Internet and e-mail; and
- Explain the consequences for individuals and the organisation if they fail to follow the rules set out in this Policy.

All users have a personal responsibility to make themselves aware of the content of the corporate security and other linked policies and to adhere to these policies.

Users must report potential breaches of security immediately to the Chief Executive Officer who will inform SCC IT managers if this is appropriate.

Any breach of the rules in this policy could result in Disciplinary Action being taken against you which could lead to dismissal. Misuses of the Internet or e-mail or a breach of the policy could also lead to civil or criminal actions against individuals or the organisation.

For those using SCC computer equipment/systems
All members of the team who are given access to SCC computer equipment/systems will adhere to the SCC ICT Policies, including the following and others that may become relevant at any time:

- Clear Screen and Desk Policy
- Corporate Information Security Policy
- Acceptable Use Policy
- Staffordshire Password Policy
- Social Networking Policy
- Privileged Access Policy

Where policies refer team to a manager in the first instance this should be the organisation's CEO who will refer issues to relevant SCC managers if needed.

Guidance on Good Practice for using non-MSN/SCC IT equipment

Passwords
- Passwords should be changed regularly
- Passwords must never be written down and displayed in your work area or any other highly visible place
- Do not talk about your password in front of others
- Do not electronically record your password or include it in an email or any written documentation
- Do not reveal a password on questionnaires or security form.
- Never share your passwords with others
- If it is necessary to give your password to IT Support staff do it verbally and change your password immediately after the work has been completed
- Passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed
- Do not let anyone observe you entering your password
- Ideally passwords should have a minimum of 8 characters
- should contain mixed case and special characters or punctuation (A to Z; a to z; 0 to 9; ! $ # % ^ @ & ( ) _ + | ~ - = ' { } [ ] < >) if the system permits e.g. "eT6^Wg%3
- must be significantly different from previous passwords
- Do not use any part of your account name
- Do not use the name of family, pet, friend, co-worker, fantasy character etc
- Do not use a word found in a dictionary (English or foreign)
- Do not use your name, initials or logon ID

- Do not use birthdays and other personal information such as addresses or phone numbers
- Good passwords include:
  - two or three short words that are unrelated e.g. “car*desk”
  - Deliberately misspelt words e.g. “sIcurEty!”
  - *use of a pass***phrase** instead of a pass***word***. Eg My cat has furry feet”. Then construct the password using the first letter of each word and add one or two non-alphabetic or numeric characters somewhere in the string. The password example may then look something like: - #mchff1.

Clear Screen / Clear Desk

Always make sure your only you can see your computer screen and that you do not leave papers laying around with participant or MSN confidential information.

Social Networking sites

PLEASE REFER TO THE SAFEGUARDING POLICY – SECTION 5: SOCIAL NETWORKING AND VIDEO SHARING WEBSITE POLICY FOR FULL DETAILS OF MAKE SOME NOISE REQUIREMENTS RELATING TO SOCIAL NETWORKS

While MSN cannot restrict the private use of social networking sites MSN expects everyone associated with the organisation to use common sense when engaging in such sites. All members of the MSN team are personally accountable for whatever they put into the public domain and inappropriate use may leave individuals subject to disciplinary procedures and/or withdrawal of contracts for misconduct.

Use of Social Media sites

Under no circumstances should personal social networking pages be used to communicate with service users or members of the public on behalf of the organisation. This will be deemed a breach of professional standards and may result in formal action.

All social networking sites, video media etc that references Make Some Noise must be approved by the Chief Executive Officer

No use of organisation logos and branding without the express permission of the CEO.

A Guide to the Legal Issues Relating to use of E-mail and the Internet

Introduction

This section of the Policy is intended to give computer users guidance on the most important legal issues which may arise from their use of the organisation’s e-mail system and Internet access.

These are not just theoretical issues. If the law is broken, then this could lead to one or more of the following consequences

- Civil and/or criminal liability for individuals and the organisation
- Disciplinary action including dismissal.

Bullying and Harassment
The organisation intends that all employees will be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or because of sex, race, disability, sexual orientation, age, religion or political beliefs.

Harassment could include sending sexist or racist jokes, making sexual propositions or abuse by e-mail. Messages containing such material must not be sent. Bullying and harassment of any kind will be treated as serious disciplinary matters which may lead to dismissal.

Breach of Copyright
Materials encountered on the Internet or received by e-mail are likely to be protected by copyright. This will apply to written materials, software, music recordings, graphics & artwork and video clips.

Only the owner of the copyright, or other persons who have the owner's consent, can copy those materials or distribute them.

If such materials are copied or amended without the copyright owner's consent, then the individual doing so may be sued for damages by the copyright owner. The organisation may also be liable, and, in some circumstances, criminal liability can arise for both the individual and the organisation.

All computer users are required to be careful not to copy text or to download software or music unless they are sure they have permission to do so; they are required to check the materials in question to see if they contain any written prohibitions or permissions before you copy or download them.

It is a criminal offence to download any software, music recordings or other materials that are known to be fakes or "pirate copies".

Unwanted Contracts
An exchange of e-mail messages can lead to a contract being formed between an individual or the organisation, and the other person. Contracts can arise easily. All that is required is the acceptance of an offer with the intention that legal obligations should arise and some payment or other consideration being made for the performance of those obligations. Breach of contract can expose the organisation to a claim for damages.

Contracting by e-mail is subject to the same requirements as any other form of contract. The organisation's established policies and procedures regarding purchasing and contracting should be adhered to.

Computer users must never commit the organisation to any obligations by e-mail without ensuring that they have the authority to do so. If computer users have any concerns that what they are doing will form a contract, they should contact the Chief Executive Officer. All e-mails relating to contractual negotiations should be marked "Subject to Contract".

E-mail users should ensure that any person with whom you wish to enter into a contract is adequately identified.

E-mail users should also beware of any attempt by the party with whom you are dealing to incorporate its own terms and conditions into a contract.

Defamation
Computer users who send an e-mail (including internal e-mail), or post any information on the Internet which contains any remarks which may adversely affect the reputation of another organisation or person, will be exposing both themselves and the organisation to the risk of legal action for defamation. This is a real risk. Other organisations have been sued for the defamatory content of e-mails sent by employees and have been required to pay out considerable sums as a result.

Obscene Material
Computer users must not under any circumstances use the organisation's e-mail system or Internet access to visit, view, display, circulate or transmit any material with a sexual content. This may constitute a criminal offence and both the organisation and individuals personally could be liable.

Protection of Personal Data
The organisation is required to comply with legislation concerning the protection of personal data. Failure by the organisation to adhere to that legislation could expose the organisation to civil liability and to enforcement action by the Data Protection authorities.

The obligations of the organisation under that legislation are complex but computer users can help ensure compliance by adhering to the following:

- Familiarity with the current version of the Data Protection Policy and Privacy Notice and how it applies to each different category of data
- Information which might be considered personal in any way must not be disclosed via e-mail or the internet
- Computer users should be particularly careful when dealing with information concerning a person's racial or ethnic origin, sexual life, political beliefs, trade union membership, religious beliefs, physical or mental health, financial matter, age, genetic, biometric and/or health data and criminal offences. Such information should only be communicated with the explicit written consent of the individual

Disposal of Removable Storage Media
Make Some Noise must ensure that all removable storage media are cleaned before being disposed of.

Responsibilities
It is the responsibility of the Make Some Noise team including Trustees, staff, volunteers, freelance workers to ensure that Removable Storage Media no longer in use is returned to Make Some Noise. It is the responsibility of the CEO acting as "Information Security Manager" to manage the secure disposal of all storage media that is no longer required, according to this procedure. The Information Security Manager can also be the owner of the relationship with the approved third-party contractor who removes shredded documents.

Procedure
1) IT hardware provided by Staffordshire County Council will be maintained and disposed of by SCC
2) IT hardware provided by Make Some Noise will be maintained and disposed of by Make Some Noise
3) The Information Security Manager shall update the Disposal Log for Removal Storage Media to evidence what storage media has been destroyed or disposed of, when and by whom.
4) Hard disks must be cleaned and verified by taking the following steps: Passed to Staffordshire County Council as our IT provider or passed to a GDPR Compliant Third Party identified by Make Some Noise. The details of the external service provider must be entered in the Disposal Log for Removal Storage Media
5) Removable storage media devices that contain confidential information must be destroyed only after a risk assessment has been carried out and must never be reused.
6) Removable storage media devices that contain confidential information must be subjected to a risk assessment before they are sent for repair in order to establish whether they ought to be repaired or replaced.
7) The protocol for destroying removable storage media devices prior to disposal is as follows: Freelance and Core team pass to Admin team. Pass to disposal company, either Staffordshire County Council or GDPR Compliant Third Party, update Disposal Log
8) All media must be disposed of according to the legal and regulatory requirements for the disposal of computer equipment, via Staffordshire County Council, Make Some Noise's approved third party.
9) Documents that contain confidential and restricted information must be placed in the secure blue boxes provided by Staffordshire County Council. The shredded waste is removed under a contract organised by Staffordshire County Council.

Monitoring, Reporting and Review

The Chief Executive Officer will ensure that Make Some Noise monitors the effectiveness of this policy through the collection and analysis of monitoring data using the tools featured in the following appendices. This data shall provide the basis of scheduled Data Protection reports to the Board of Trustees and subsequent reviews of this policy.

RELEVANT LEGISLATION

- Data Protection Act 1998
- General Data Protection Regulations
- General Data Processing Regulations (GDPR May 2018)
- Child Protection Legislation (including but not limited to Children Act 1989, Children Act 200, Safeguarding Vulnerable Groups Act 2006)
- DSE Regulations
- Copyright, Designs and Patents Act 1988

Forms referred to in this Policy

- Disposal Log for Removal Storage Media

Linked Policies

- Data Protection Policy (including Privacy Notice)
- Safeguarding Policy
- Health and Safety Policy
- Disciplinary Policy
- Bullying and Harassment
- Grievance
- Whistleblowing Policy

FURTHER INFORMATION

- SCC Intranet for ICT Policy
- MSN Policy file
- Health & Safety Executive (http://www.hse.gov.uk)
- ACAS (http://www.acas.org.uk)
- NSPCC (https://www.nspcc.org.uk/preventing-abuse/child-protection-system/england/legislation-policy-guidance/)
- http://www.legislation.gov.uk/browse