Reaching People

Commitment to
Lasting Change

ICT Policy

October 2018

1. Introduction

This policy sets out the expectations on employees of our organisations including contractors and temporary staff, who use the organisation’s IT facilities. IT facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them. All users are responsible for IT activity which is initiated under their username.

This policy should be read in conjunction with other Reaching People policies and in particular, the following:

- Code of Conduct
- Confidentiality Policy
- Data Protection Policy
- Safeguarding Policies

2. Legislation

All users shall comply with the relevant legislation. This includes the following:

- Data Protection Act 1998/Freedom of Information Act 2000
- Computer misuse Act 1990
- Copyright Design and Patents Act 1998
- Defamation Act 1996
- Terrorism Act 2006
- *Telecommunications (Lawful business Practice) (Interception of Communications) Regulations 2000*

3. Authorisation

No person is allowed to use the organisations IT facilities who have not previously been authorised to do so. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

4. Passwords & Work Station Security

Access to Reaching People’s computer systems is secured by user passwords. Passwords must not, under any circumstances be given, or made available to others. If an ICT user suspects their password has been compromised, they must change it at once and report this to the Resources & Communications Coordinator who will help reset the password where necessary.

To prevent unauthorised access to our systems, you are required to lock your computer each time you are away from your desk. For periods of absence in excess of one hour, you are required to log off the system. If your computer is locked and an administrator unlocks your station, you will lose any unsaved work. Therefore, you must ensure you save any work prior to locking or logging off your work station.

Any documents which contain sensitive data (either for individuals or organisations) must be password protected.

5. Use of the Internet

Use of the Internet is encouraged where such use is consistent with a person's work and with their goals and objectives of the organisation in mind. Reasonable personal use is permissible subject to the following:

a) Users must not participate in any online activities that are likely to bring the organisation into disrepute. If you are uncertain about this, please speak to your line manager.
b) Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material.
c) Users must not knowingly introduce any form of computer virus into the Organisation's computer network.
d) Users must not download commercial software or any copyrighted materials belonging to third parties.
e) Users must not use the internet for personal financial gain, nor for illegal or criminal activities, such as software and music piracy, terrorism, fraud, or the sale of illegal drugs;
f) Users must not use the internet to send offensive or harassing material to other users.
g) Use of the Internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and done only during non-work time such as lunch time.

6. Good Practice

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for. Use of charity log for sending confidential information between partner delivery organisations preferred where possible. Emails containing confidential information should be password protected.

Reaching People provides a current and up to date automatic virus checker on its computers, however caution must be used when opening any attachments or emails from unknown senders. Users must user their best endeavour to ensure that any file downloaded from the internet is done from a reliable source. It is a disciplinary offence to disable the virus checker. Any concerns about external emails, including files containing attachments, must be discussed with your line manager.

7. Social Media

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media.

Employees are only permitted to log on to social media websites using the organisation's IT systems and equipment outside their normal working hours, (for example, during lunch breaks or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. This includes use of laptop and hand-help computers or devices distributed by RP for work purposes. We nevertheless reserve the right to restrict access to these types of websites at any time. Where employees have their own computers or devices, such as laptops and handheld devices, again they must limit their use of social media on this equipment to outside their normal working hours.

Employees and staff of member organisations may be asked to contribute to the organisation's social media activities during normal work hours as part of their work role. All staff must be aware at all times that, while contributing to our social media activities, they are representing Reaching People and all media interactions must be in line with Company policy.

8. Organisational Social Media Activities

Where employees or RP or member organisations are authorised to contribute to Reaching People social media activities as part of their work, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

a) Follow the Code of Conduct
b) Ensure that any communication has a purpose and benefit the organisation
c) Obtain permission from their line manager before embarking on a public campaign using social media
d) Follow all organisation policies and procedures, in particular, ones highlighted at the introduction to this policy.
f) Follow any additional guidelines as given by Reaching People from time to time

9. Personal Social Media Rules

We recognise that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of us, in these circumstances, all staff must be aware that their actions may reflect on Reaching People if they are recognised online as being one of our employees or connected with Reaching People via their own organisation. The following social media rules have been put in place to protect both staff and the organisation.

When logging on to and using social media websites and blogs at any time, employees and members' staff must not:

a) Write about their work for RP other than in relation to RP's own social media activities or where expressly permitted by us on business networking websites such as LinkedIn.
b) Use their work email address when registering on such sites or provide any link to our website other than in relation to our own social media activities where expressly permitted by us on business networking websites such as LinkedIn
c) Include personal information, including photographs or data about our employees, member organisations, service users, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees and clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as we reasonably believe they are identifiable) – this could constitute a breach of the Data Protection Act 1998.

d) Disclose any trade secrets or confidential, proprietary or sensitive information belonging to RP, its members, service users, customers, contractors or suppliers or any information which could be used by one or more of our competitors, for example information about our work, products and services, technical developments, or current and future business plans.

e) Breach copyright or any other proprietary interest belonging to RP. (See data protection and copyright policies for further information).

f) Post any other company information other than positive promotion.

Employees/other members' staff must remove any content immediately if they are asked to do so by us.

Work and business contacts made during the course of employment through social media websites and which are added to personal social networking accounts amount to confidential information belonging to the Organisation and accordingly must be surrendered on termination of employment by surrounding the account password on termination of employment.

All staff must remember that social media websites are public and that use of restricted access settings does not guarantee posting on any website will remain private.

Should a staff member notice any inaccurate information about RP online, they must report this to their line manager in the first instance.

10. Network Drives and Storage Standards

Local C: drives must not be used for storing any business related data, as in the event of hard drive failure, the information will not be backed up and will potentially become, irretrievable.

Permission must be sought from line management to store organisational data on any external storage devices.

11. Cloud Computing

Cloud Computing is an on-demand self-service Internet infrastructure which allows internet users access to online storage, services and online programs via an internet browser. With the exception of Charity Log, the use of cloud computing is not permitted for the normal use and distribution of work files as it lacks the necessary security and data protection protocols. Cloud Computing must only be used for public documents such as training programmes, leaflets, event invitations, public photos and presentations and must be restricted to specific authorised services. (Appendix 3).

12. Loss or theft of hardware or data

All users issued with hardware must to be conscious of the security of the equipment and data stored on it at all times. As such, no personal data is to be kept on hardware issued by RP. These devices must not be left in a public place where they can be stolen or damaged and confidential organisation information viewed by unauthorised parties.

In the event that any device is lost or stolen, or in the event that passwords for cloud computing have been compromised, the user must contact the CEO as soon as possible and explain what has happened so measures can be taken to protect the systems.

13. Remote Users

Users may sometimes need to use Organisation equipment and access the Organisation network while working remotely, whether from home or while travelling. The standards set out in this document apply equally when using equipment or resources other than that provided by us.

14. Monitoring

All resources, including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of normal business activity then, at any time and without prior notice, we maintain the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised personnel only. Any information stored on a computer, whether the information is contained on a hard drive, USB pen or in any other manner may be subject to scrutiny by us. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

15. Social Media Monitoring

We reserve the right to monitor employees' use of social media on the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- Promote productivity
- Ensure the security of the system and its effective operation
- Make sure there is no unauthorised use of the our time
- Ensure that inappropriate, restricted or blocked websites are not being accessed by employees
- Make sure there is no breach of confidentiality or this policy
- We reserve the right to restrict, deny or remove internet access, or access to particular social media websites, to or from any employee

16. Penalties for Improper Use

Withdrawal of facilities

Users in breach of these regulations may have access to our IT facilities restricted or withdrawn.

Disciplinary Action

Breaches of these regulations will be dealt with under our disciplinary procedures. It may lead to termination of employment.

Breaches of the law

Applicable breaches of the law will be reported to the police.

17. Account Closures

When a member of staff is due to leave the organisation, they will be requested to ensure that all work-related computer filing is completed and files remain accessible to their line manager. At a pre-determined time, their IT account and related email accounts/passwords will be terminated by the organisation.

18. Use of own personal I.T equipment

Ensuring all personal I.T equipment used for work purposes is virus protected and up to date it is permitted. The personal I.T equipment usage form for work is required to be completed. And a copy logged on your personal file.

19. Contravention of this Policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and will result in disciplinary action being taken under the Organisation's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Document Control

Approved by:		
Signature:		
Board Responsibility:		
Review Date:	October 2020	

Personal I.T Equipment for work usage form

I confirm the personal I.T equipment used for work purposes is supported with up to date Virus protection and details are confirmed below:

Name of Virus protection software____

____

Date of coverage/Expiry____

Signed (Staff Member)____

Print____

Authorised Cloud Services

Information & Communications Technologies Policy

Definition

Cloud Services are an on-demand self-service Internet infrastructure which allows internet users access to online storage, services and online programs via software.

The use of cloud services is not permitted for the normal use and distribution of work files as it lacks the necessary security and data protection protocols.

Cloud Services should only be used for public documents such as training programs, leaflets, event invitations, public photo's and presentations and should be restricted to specific authorised services

LASS's Requirements to use cloud services may change from time to time and this list will be updated to account for changes as and when necessary. Employees will be informed when authorised services have changed but it is their responsibility to read the latest version of this document.

Facebook **(http://www.facebook.com/pages/LASS/106385432763026)**

Used to reach to individuals who use Facebook on a regular basis. Events, news feeds, images and video may be displayed. Social interaction is not permitted through facebook.

YouTube (http://www.youtube.com/user/lassleicester)

Used to upload video content which can then be embedded into out website. Social interaction is not permitted through YouTube however, videos and playlists may be 'liked' and added to the account favorites.

Twitter (**http://twitter.com/#!/lassleics**)

Used to advertise news articles, stories or LASS Events which appear on our website. In every instance, a link the LASS's website must be displayed. The "Tiny" service ***(http://tiny.cc/)*** is used to shorten urls and statistics are available from these links.

Google Analytics (https://www.google.com/analytics)

Used to provide statistics and analytics for our website.

Flickr (http://www.flickr.com/)

Flickr is an image and video hosting website and web services suite. Flickr is used to host images for entry on our website and blogging services (where appropriate).

WordPress.com (http://wordpress.com/)

WordPress.com is a WordPress Multi-User weblog hosting provider. It is used as a web presence for Well For Living: ***www.wellforliving.co.uk.***