Springboard Opportunity Group

ICT Acceptable Use Policy

This policy should be read in conjunction with other policies, especially Data Protection, Retention & Storage of Documents and Equality & Diversity.

This policy defines acceptable use of for all Information and Communication Technology (ICT) provided by Springboard Opportunity Group and used by staff for their work, volunteers and others using our ICT facilities.

ICT includes phones, PCs, laptops, tablets, cameras, photocopiers, tv screens, data sticks and drives, printers and services such as email and internet access including online learning diaries, social media, website and all other digital media.

Newer technologies are integral to ensure the smooth running of an organisation and Springboard values the impact of ICT on our work and aims to optimise its use for all aspects.

To achieve this we will follow good practice guidelines with regard to the all aspects of its operation.

E-Safety for children

Children at Springboard will always be supervised when using ICT equipment. Where children may have access to iPads, tablets or computers, the setting Manager must ensure:

- highest levels of parental controls are in place at all times.
- downloaded games and activities are from reputable sites
- staff awareness of the existence of safe search engines
- safe-search settings on Youtube and Google are activated

Acceptable Use

Staff may use Springboard Opportunity Group's ICT facilities to carry out any activity that is part of their role or as directed by their line manager. It is essential that staff increase their use and knowledge of ICT for work purposes and will be encouraged and expected to develop their skills.

Staff may use Springboard ICT facilities in moderation for their personal use provided that

- it does not impact on their work
- no additional cost is incurred by Springboard
- it does not break the law e.g. inappropriate material or illegal sites
- it is not for personal financial gain e.g. online auction sites; gambling; political purposes; advertising.

- it does not contravene the conditions set out in this policy

Unacceptable use

The organisation's ICT may **not** be used for any of the following:

- mobile phones must not be used for taking photographs
- iPads are not to be used for outings in case of theft or loss.
- deliberately accessing, creating or transmitting material that is offensive, hateful, defamatory, obscene, indecent, or likely to cause annoyance, inconvenience or other needless concern
- using material which infringes the copyright of another person or organisation
- attempting to gain unauthorised access to ICT facilities or services, or to confidential material e.g. by unauthorised use of a password
- loading software including programs, games, messaging services or other material unless duly authorised by a line manager.
- modifying hardware e.g. by adding or removing components.
- changing software settings e.g. to antivirus, backup software or by creating unnecessary user accounts.
- changing access passwords unless duly authorised by the ICT Lead and recorded

Additionally:

- security details including passwords must not be given to unauthorised people.
- users should normally log out if they are going to be away from their PC for any length of time
- all equipment must be switched off at the end of the day unless otherwise instructed.
- any unusual error messages or concerns must be reported to ICT lead
- care must be taken of all equipment.
- careful consideration should be given before downloading e.g. music, films; as this may slow down computer use for other users.
- documents should be stored on NAS within the Springboard framework overseen by Business Manager
- Springboard mobile phones are provided to several staff and each setting. They must be used only for Springboard business
- Staff may choose to use their own personal mobile phones for Springboard business related to their role, but must not use it to contact parents/carers.
- Personal phone numbers must not be given to parents/carers.
- Personal email addresses must not be used to contact parents/carers or external agencies.
- All staff who require a Springboard email address will be given one.

Legal Implications

It is important to be aware of relevant legislation and regulations and the consequences that could arise from the misuse of Springboard ICT. This could result in prosecution. These include:

- Data Protection: e.g. failing to adequately protect personally identifiable information or inappropriate marketing using personal information
- Charities Law: e.g. failure to meet financial reporting requirements because of system break down or inadequate back up
- Equalities legislation: e.g. failure to provide suitable ICT equipment or make reasonable adjustments to the website
- Health and Safety: failure to provide suitable ICT equipment or allow users to take adequate breaks
- Software licensing and copyright: e.g. using unlicensed software, using copyright material without permission
- Libel laws: e.g. libellous or defamatory material sent by email or posted to internet sites
- Computer Misuse Act 1990: attempting to gain unauthorised access to information or facilities

Security and Confidentiality

ICT equipment is valuable in itself and for the information it contains. Each piece of equipment will have a code and marked with a UV pen.

Reasonable steps will be taken to ensure the safety and security of all ICT equipment at premises owned / rented by Springboard. This includes locking premises, shutting down equipment when not in use and locking away portable items.

Staff removing equipment from the premises are responsible for its security and safe return and for ensuring it is not used or contents accessed by non-authorised people

If confidential or sensitive information is taken off the premises electronically, a password must be added.
Springboard information can be kept on memory sticks or laptops, but only for training or similar purposes. It must not be of a sensitive nature such e.g. a child's file or unauthorised photos and must be deleted if no longer needed.

When work is undertaken on such documents e.g. on home computers, the member of staff is responsible for ensuring that this is not seen by any other person and that the information does not remain on their own computer, laptop etc.

A record of ICT equipment will be maintained (larger / more expensive items will be listed on the inventory), and security marked for insurance purposes.

Due regard will be given to material displayed on screen to ensure it cannot be seen by unauthorised people. This includes the use of screen savers and closing down confidential information when others might see it.

Computers and laptops will be backed-up remotely every day, by Springboard's ICT consultants.

All photos and videos are to be downloaded from iPads and cameras to a pc from other equipment every week and then deleted from the mobile equipment.

A schedule for system maintenance and security will be implemented.

With parental consent and following rules of recipient, personal information about children e.g reports can be e-mailed. Full names of children may be used but care must be taken to ensure that information is sent only to the intended recipients.

Unless there is good reason not to do so, parents registered with Springboard should be copied in on emails sent about their children.

Purchasing and use of equipment and software

Equipment and software will be purchased in line with normal requisition procedures.

Software installed on Springboard computers is licensed to Springboard and may not be installed on other computers, such as a member of staff's home computer unless this is permitted under the license and then only with the agreement of Springboard.

There is a named member of staff responsible for ensuring necessary safeguards e.g. firewalls are installed and maintained.

This policy was adopted by Springboard Opportunity Group's Board of Trustees	
Date of meeting	29.01.19
Date to be reviewed:	January 2022
Signed on behalf of the Board of Trustees	
Name of signatory	Louise Petersen
Role of signatory	Chair