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 but is not limited to; 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

Internet access

- Children never have access to the internet.
- Only apps that can be downloaded and used without internet access are used by children.
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- All computers for use by children are sited in an area clearly visible to staff.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

tablets

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not used by playroom staff during working hours. This does not include breaks where personal mobiles

may be used off the premises or in a safe place e,g, staff room. The setting manager completes a risk assessment for where they can be used safely.

- Personal mobile phones of playroom staff are switched off and stored in lockers or a locked office drawer.
- In an emergency, personal mobile phones may be used in the privacy of the office with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

Use of social media

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure the organisation is not negatively affected by their actions and do not name the setting
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- are aware that images, such as those on Snapchat may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to access
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or breaches to the designated person in their setting

- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed
-

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:

- 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 other application 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. IT equipment will be locked when user is away from the screen i.e. locked screens.

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 temporarily stored on memory sticks or laptops, but must be password protected 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.

The NAS is backed up remotely 5X per week by IT consultants
All photos and videos are to be downloaded from tablets 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	March 2022
Date to be reviewed:	January 2025
Signed on behalf of the Board of Trustees	
Name of signatory	Elizabeth Manning
Role of signatory	Chair of Trustees