# 

Online security (e-safeguarding) Policy

## Introduction

Springboard recognises that the use of Information and Communication Technology (ICT) is essential to modern life and an integral part of our modus operandi. However, we also recognise that technology brings with it potential dangers. Indeed, as the technology evolves, so too do the dangers. We cannot foresee future developments, and so any ICT policy inevitably will be reactionary. It is our intention, within that caveat, to be as up to date as possible[[1]](#footnote-1).

An Online Security Policy (e-safeguarding) is the first line of defence in managing security on Springboard’s IT Systems. The security risks are generated by users, sometimes intentionally but more often than not because they are unaware of the potential risks involved with Internet based communications.

The purpose of this policy is to make certain that all users understand the requirements that are necessary to ensure all users are protected and our data remains secure. Compliance with the regulations outlined in this policy is the responsibility of all members of the Springboard community and will be enforced by IT Services.

The communication to all users of the requirements of this policy is mandatory. New staff employed by Springboard will have this conveyed to them upon their initial induction and will be required to sign a declaration to confirm agreement and understanding. Learners joining a Springboard programme will also follow a similar procedure and sign a declaration of acceptance.

Access to Internet based communications will only be granted upon the signing of these agreements.

## Purpose

The purpose of this policy statement is to:

1. To ensure that everyone is familiar with what procedures are regarded as unacceptable

IT services has developed this policy for the use of computers, which prohibits all users from abusing the system. This policy outlines what is expected from all persons involved in ‘computer related communications’ and provides information about what ‘is’ and what ‘is not’ considered acceptable use. This policy applies to all Springboard employees or representatives and to those trainees and members of the public offered access to company ICT facilities at each Springboard delivery site.

1. Ensure the safety and wellbeing of young people, adults and staff using the internet, social media or mobile devices.

This policy will help protect learners, staff and the organisation by clearly stating what is acceptable and what is not. We may exercise our right, by electronic means, to monitor the use of Springboard’s computer systems, including the monitoring of web sites visited and emails sent: the ICT Manager will coordinate this.

1. Provide staff and volunteers with the overarching principles that guide our approach to online safety

Springboard does not attempt to “lock down” access to the Internet, but rather to manage and filter the services provided to an appropriate degree. We also understand that it is possible that learners and staff could access the Internet using methods that cannot be managed or filtered by them e.g. by using cellular data (for example a 4G connection via a mobile phone). Springboard believes that it is vital to educate learners, staff and management as to the possible risks that may be encountered online, and what to do if there is a problem.

1. Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices

The Internet and related online activities can be a distraction and a temptation to spend valuable time on non-business, non-educational or non-vocational activities. Use of the Internet is permitted and encouraged where such use is educational and complements current learning aims on Springboard programmes or supports the goals and objectives of the Trust and its business. The Internet and related online activities such as e-mail should be used in a manner that reflects the company’s current standards and codes of conduct

## Roles and Responsibilities

We believe that online safety (e-safeguarding) is the responsibility of the whole Springboard community, and everyone has a responsibility to ensure that all ICT users are able to benefit from the opportunities that technology provides for teaching and learning. The following responsibilities demonstrate how each member of the community will contribute.

### Senior Management Team

* The Chief Executive has overall responsibility for e-safeguarding all members of the Springboard community, though the day to day responsibility for e-safeguarding will be delegated to the ICT Manager and the IT Services team.
* The Chief Executive and Senior Management Team are responsible for ensuring that the ICT Manager and other relevant staff receive suitable training to enable them to carry out their e-safeguarding roles and to train other colleagues when necessary.
* The Chief Executive and Senior Management Team should ensure that they are aware of procedures to be followed in the event of a serious e-safeguarding incident.

### Safeguarding Committee

* To ensure that Springboard’s e-safeguarding policy is current and pertinent.
* To ensure that Springboard’s e-safeguarding policy is systematically reviewed at agreed time intervals.
* To ensure that Springboard’s Acceptable Use Policies are appropriate for the intended audience.
* To promote to all members of the Springboard community the safe use of the internet and any technologies deployed within the organisation.

### ICT Manager and IT Services team

* To promote an awareness and commitment to e-safeguarding throughout the entire organisation.
* To take day-to-day responsibility for Springboard’s e-safeguarding and to have a leading role in establishing and reviewing the e-safeguarding policies and procedures.
* To develop an understanding of current e-safeguarding issues, guidance and appropriate legislation.
* To ensure that all members of staff receive an appropriate level of training in e-safeguarding issues.
* To monitor and report on e-safeguarding issues to the Safeguarding committee and the Senior Management Team as appropriate.
* To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safeguarding incident.
* To ensure that access controls exist to protect personal and sensitive information held on Springboard-owned devices.
* To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within Springboard delivery sites.

### Teaching and Support Staff

* To read, understand and help promote the Springboard’s e-safeguarding and Acceptable Use policies and guidance.
* To report any suspected misuse or problem to the ICT Manager or Head of Performance as appropriate.
* To develop and maintain an awareness of current e-safeguarding issues and guidance.
* To model safe and responsible behaviours in their own use of technology and maintain a professional level of conduct in personal use at all times.
* To ensure that any digital communications with learner should be on a professional level and only through Springboard based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
* To embed e-safeguarding messages in learning activities across all areas of the curriculum.
* To supervise and guide learners carefully when engaged in activities involving technology.
* To ensure that learners are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
* To be aware of e-safeguarding issues related to the use of mobile phones, cameras and handheld devices.
* To understand and be aware of incident-reporting mechanisms that exist within Springboard.
* Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

### Internet Service Providers, External Support agencies

* To support the ICT Manager and IT Services team with the deployment and management of server based and endpoint security software.
* To support Springboard in providing a safe technical infrastructure to support teaching and learning across all delivery locations.
* To ensure that external access to Springboard’s computer network is only through an authorised, restricted mechanism.
* To support the ICT Manager and IT Services team to ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

## Guidance for Learners

New technologies have become integral to the lives of children and young people in today’s society, both within education and in their lives outside Springboard. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This policy is intended to ensure:**

* that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that Springboard ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. Springboard will try to ensure that learners will have good access to ICT to enhance their learning and will, in return, expect the learners to agree to be responsible users.

**Learner Agreement Policy**

I understand that I must use Springboard ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

* I understand that that Springboard will monitor my use of the ICT systems, email and other digital communications.
* I will not share my username and password with anyone or try to use any other person’s username and password.
* I will be aware of “stranger danger”, when I am communicating on-line.
* I will not disclose or share personal information about myself or others when on-line.
* If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take someone else with me.
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology to support our education:

* I understand that Springboard ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
* I will not use Springboard’s ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing.

I will act as I expect others to act toward me:

* I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will not take or distribute images of anyone without their permission.

I understand that Springboard has a responsibility to keep the technology secure and safe:

* I understand that I do not use my own devices at Springboard without prior permission.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
* I will immediately report any damage or faults involving equipment or software; however this may have happened.
* I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
* I will only use chat and social networking sites with permission and at the times that are allowed and supervised.

When using the internet for research for my course work, I understand that:

* I should ensure that I have permission to use the original work of others in my own work.
* Where work is protected by copyright, I will not try to download copies (including music and videos).
* When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

I understand that I am responsible for my actions, both in and out of Springboard:

* I understand that Springboard could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, whether at Springboard or outside. Examples of this is cyberbullying, sending/receiving inappropriate images and misuse of personal information.
* I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action. This may include loss of access to the network / internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in this policy agreement. If you do not sign and return this agreement, access will not be granted to Springboard ICT systems.**

## Leaner Agreement Form

This form relates to the learner Agreement Policy. Please complete the sections below to show that you have read, understood and agree to the rules included in the Agreement. If you do not sign and return this agreement, access will not be granted to Springboard ICT systems.

I have read and understand the above and agree to follow these guidelines when:

* I use the Springboard ICT systems and equipment
* I use my own equipment at Springboard (when allowed) e.g. mobile phones, cameras etc.
* I use my own equipment outside of Springboard in a way that is related to me being a member of the Springboard community e.g. communicating with other Springboard learners through social networks, mobile phones, accessing email, Learning Platform, websites etc.

1. Changes will be made immediately if technological or other ICT developments so require. [↑](#footnote-ref-1)