



e-Safety Policy

Introduction

TheLightBulb is committed to providing a quality enriched learning journey and we recognise the benefits and opportunities which new technologies offer to teaching and learning. We provide access to ICT systems and internet to staff and, where appropriate, learners/apprentices and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

We will implement, and monitor the effectiveness of, appropriate safeguards within the centre while supporting staff and learners/apprentices to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. We will do all that we can to make our learners/apprentices and staff stay e-safe and to satisfy our duty of care. This e-safety policy should be read alongside other relevant centre policies including but not limited to: Prevent, Internet and Email Usage, Social Media Usage, Learner Safeguarding and Anti-Harassment policies.

Development and review

TheLightBulb involved the whole organisation in the writing of the e-safety policy through team meetings, training sessions and activities.

Review of the policy will take place bi-annually or more frequently, in response to, significant developments in the use of technologies, which will impact the organisation and its learners/apprentices, new threats to e-safety or any serious incidents, should they occur.

Policy Scope

The policy applies to the whole organisation, including staff, associates, learners/apprentices and employers who have access to and are users of centre ICT systems, and/or expected to use ICT as part of their qualification with TheLightBulb, both in and away from the centre. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email and mobile phones.

Roles and Responsibilities

All staff are responsible for ensuring the safety of learners/apprentices and should report any concerns immediately to their line manager and/or designated e-safety officer. Any report of an e-safety incident will be dealt with in accordance with the organisation's learner safeguarding policy.

The designated e-safety officer is:

Suzanne Tilling
01268 270648
suzanne@thelightbulb.net

In the absence of the e-safety officer, please contact the designated safeguarding officer:

Andrea Gregory
Health & Safety Officer
001268 270648
andrea@thelightbulb.net

In the event of the above being absent then please contact **Lesley Jones** (Managing Director) on 01268 270648.

e-Safety Officer:

The e-Safety Officer is responsible for keeping up to date with new technologies and their use, as well as maintaining CPD. They will be expected to complete, review and update the e-Safety Policy, deliver staff development and training, record incidents and report any developments and incidents to the company directors.

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021 Next Review Due April 2022	Rev. No. 6	Reviewer's Initials: SJT
\\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc			



e-Safety Policy

Learner:

Learners/apprentices are responsible for using TheLightBulb’s IT systems, where appropriate, in accordance with the organisation’s e-Safety rules and Digital Values, as described in the Learner Induction pack, which they must sign at the time of induction. Learners/apprentices must act safely and responsibly at all times when using the internet and/or mobile technologies. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another learner or member of staff.

Staff

All staff are responsible for using TheLightBulb’s IT systems and mobile devices in accordance with the company’s PREVENT Internet & Email Usage policy, Social Media Usage policy and the e-Safety Rules and Digital Values included within this policy, which they must sign and submit to the e-Safety Officer. Staff are responsible for attending staff training on e-safety and displaying a model example to learners/apprentices at all times through embedded good practice.

Online communication with learners/apprentices is restricted to the company network. External platforms not hosted by TheLightBulb, such as e-portfolio systems, may be used only where a risk assessment form has been completed by the e-safety officer and approved by the company directors.

All staff should apply relevant company policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the e-Safety Officer and/or line manager without delay.

Appropriate Behaviour

TheLightBulb will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners/apprentices should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with legal requirements and the relevant company policies.

Security

TheLightBulb will do all that it can to make sure the company IT network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of TheLightBulb systems and information. Digital communications, including email and internet postings, over the company network, will be monitored in line with the Internet and Email Usage policy.

Risk Assessment

In making use of new technologies and external online platforms, the e-safety officer must first carry out a risk assessment for e-safety. This consists of a series of questions on the suitability of the technology as well as a section in which they can record any relevant comments or evidence generated. All forms must be submitted to the company directors for their consideration and approval

Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners/apprentices.

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021	Rev. No. 6	Reviewer’s Initials: SJT
	Next Review Due April 2022		
\\\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc			



e-Safety Policy

All learners/apprentices and staff will receive training on the appropriate use of images, as well as the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.

Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

Photographs of activities on the college premises should be considered carefully and have the consent of the company directors before being published to the internet or used for marketing purposes.

All learners/apprentices must complete a photo/video consent form where their image is to be used for marketing purposes and/or published to the internet.

Personal Information

TheLightBulb collects and stores the personal information of learners/apprentices and staff in accordance with the Data Protection Act and the company’s Data Protection policy.

No personal information can be posted to the company’s website without the approval of a Director and unless it is in line with our Data Protection Policy. Only names and work email addresses of staff, where applicable, will appear on the company website. No staff or learners/apprentices’ personal information will be made available on the website without consent.

Staff must keep learners/apprentices’ personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Every user of IT facilities is required to log off or lock their computer where they are physically absent from a device for any period.

All company mobile devices such as laptops, are required to be password protected and signed out by a member of the IT team before leaving the premises, using an Equipment Sign Out form. Where equipment is allocated to an employee for their duration of employment, the employee is required to complete a Staff Equipment Form.

Where the personal data is no longer required, it must be securely deleted in line with the Data protection and retention policy.

Education and Training

With the current unlimited nature of internet access, and ever changing technologies, it is impossible for TheLightBulb to eliminate all risks for staff and learners/apprentices. It is our view therefore, that the company should support staff and learners/apprentices stay e-safe through regular updates. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners/apprentices

Learners/apprentices will receive e-safety training as part of their induction to their qualification. Where updates and new technologies are introduced, these will be communicated to all affected learners/apprentices. TheLightBulb’s Digital Values and reporting procedures will appear on the home screen when learners/apprentices access TheLightBulb’s e-portfolio system for them to view at any time and will be embedded into the learners/apprentices’ Induction pack.

Within teaching, learning and assessment, learners/apprentices will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly. They must not use the internet

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021	Rev. No. 6	Reviewer’s Initials: SJT
	Next Review Due April 2022		
\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc			



e-Safety Policy

to incite others to view radically motivated websites.

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021	Rev. No. 6	Reviewer's Initials: SJT
	Next Review Due April 2022		
\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc			



e-Safety Policy

For staff

Staff will receive updates when new technologies are introduced and as appropriate throughout the year. This will be led by the e-Safety Officer and will take the format of a workshop, allowing staff hands-on experience. Further resources of useful guidance and information will be issued to all staff following the session. Each member of staff must record the date of the training attended on their CPD/training plan. They will also receive a certificate of attendance.

Any new staff will receive e-safety training, where appropriate, led by the e-safety Officer or other designated person, and full training on the company IT system by an appropriate person. They will also be provided with a copy of the company handbook, as part of their terms and conditions of their contract, detailing all policies mentioned throughout this document.

Associate staff will be invited to attend training provided by TheLightBulb. If they are unable to do so they must provide evidence of their own CPD in this area.

Digital Values

TheLightBulb has compiled a set of e-Safety rules, our 'Digital Values' from training and consultation sessions. These have been built into the learner Induction pack as well as being displayed on our e-portfolio system. These have been agreed by, and communicated to, all staff.

We expect our staff and learners/apprentices to:

- **Protect passwords**
- Ensure passwords are strong and not shared with anyone
- **Have clear boundaries**
- Maintain boundaries between personal and professional lives and activities
- **Share information cautiously**
- Nobody's information should be shared without their permission
- **Respect ownership rights**
- Observe copyright and referencing rules
- **Think before we post!**
- Act with integrity and have respect for others in online communities including Facebook, Twitter and LinkedIn
- **Think before we type!**
- Only use professional and appropriate language in all communication. Ensure nothing we write is open to misinterpretation
- **Think before we click!**
- Not download anything or open any link unless we are confident that it is safe
- **Stick to policy**
- Follow company guidelines for personal use of ICT and social media
- **Report it!**
- Inform the e-safety officer of any incidents and/or concerns
- **Be committed to improve**
- Display commitment to improving digital literacy skills and keep up to date with changes to e-safety requirements and new technology

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021	Rev. No. 6	Reviewer's Initials: SJT
	Next Review Due April 2022		
\\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc			

e-Safety Policy

Incident reporting

Where an e-safety incident is reported to TheLightBulb, this matter will be dealt with very seriously and in accordance with the reporting procedure.

The company will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their assessor, tutor or to the company e-safety Officer. Where a member of staff wishes to report an incident, they must contact their line manager or e-safety officer as soon as possible. Following any incident, the company will review what has happened and decide on the most appropriate course of action. External agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Incidents should be reported using the e-safety incident report form and submitted to the e-safety officer for review. The e-safety officer will log all incidents reported.

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021 Next Review Due April 2022 \\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc	Rev. No. 6	Reviewer's Initials: SJT
---	--	------------	--------------------------



e-Safety Policy

E-safety Risk Assessment form

Site	Use	Who will access	Risk (low, medium, high)	Any other comments
Skills Forward (Forskills)	Support learners/apprentices with Functional Skills delivery	Delivery staff and apprentice learners/apprentices will access via a webpage.	Low	
Learning Assistant	Upload and assessing of learners/apprentices work.	Delivery staff and apprentice learners/apprentices will access via a webpage.	Low	
Facebook	Publicise and promote TLB through social media	Emily Casson	Low	
Linkedin	Publicise and promote TLB through social media	Suzanne Tilling, Emily Casson	Low	
Workstar	To track learners/apprentices soft skills for start to end point of training		low	
Padlet	Used as a postit sharing page for staff and learners/apprentices	Emily Casson Staff and learners/apprentices will access a read only webpage.	low	
Bitly	Track individual site traffic	Emily Casson	Low	
Dictionary.com	All staff and learners/apprentices encouraged to download from App store and iTunes	All staff and learners/apprentices	Low	
Twitter	Publicise and promote TLB through social media	Emily Casson	low	
City and Guilds Evolve Walled Garden	Access to register and gain learner results	Suzanne Tilling, Nicola Wilkinson, Emily Casson	low	
Pearsons EDI Edexcel	Access to register and gain learner results	Suzanne Tilling, Nicola Wilkinson, Emily Casson	low	

Responsible person Suzanne Tilling Managing Director	Revision Date 12/04/2021 Next Review Due April 2022	Rev. No. 6	Reviewer's Initials: SJT
	\\dcf01\Admin\Matthew Smith\Matts work\Website\Policies & Procedures\Policy - E-Safety v6 12 04 2021.doc		

