THE LEARNING FOUNDRY

E-Safety and Social Media Policy

Overview:	**This policy is to govern and guide on the use of the internet, social media and all other forms of e-communication and is aimed at any person who is undertaking any form of learning with The Learning Foundry, known as Learners, and employees of The Learning Foundry, known as Colleagues.**
Approved by:	**TLF Management Team/Board**
Date approved:	**March 2018**
Next review date:	**March 2020**
Champion:	**Managing Director**
Lead:	**Quality and Performance Manager**

1. Introduction/ policy statement

1.1 The Learning Foundry invests in colleagues being able to support learners in the use of technology and online services. Each colleague has a responsibility to ensure that our learners are kept safe. Overarching the E-safety policy is The Learning Foundry's Safeguarding Policy.

1.2 This policy aims to:

- Educate learners about E- safety issues and appropriate behaviours so that they remain safe and legal online.
- Help learners to develop critical thinking skills to reflect and enable them to keep themselves safe.
- Keep any personal data and information secure.
- Minimise the risks of handling sensitive information.
- Ensure that all colleagues and learners comply with the policies of The Regenda Group.
- Outlines key contacts, roles and responsibilities as well as defining what safeguarding means and the actions The Learning Foundry and our partner organisations will undertake to address any potential incidents or issues.

1.3 The Learning Foundry's E-safety policy runs in conjunction with the

- The Learning Foundry's Safeguarding Policy
- The Learning Foundry's Code of Conduct
- Regenda Group Information Security and Systems Usage Policy

2. Scope and exemptions

2.1 This policy applies to The Learning Foundry, a wholly owned subsidiary of Regenda Homes, which is part of The Regenda Group.

2.2 Tutors and Assessors are responsible for monitoring and E-Safety education within their lessons and support sessions.

3. Definitions

3.1 Learner: any person who is undertaking any form of learning with The Learning Foundry.

3.2 Colleagues: employees of The Learning Foundry.

4. Policy detail

4.1 At The Learning Foundry we will ensure that we meet the statutory obligations to keep learners safe and protected from potential harm by understanding consequences of misuse.

4.2 All internet access at The Learning Foundry sites is filtered. We endeavour to block unsuitable sites. However, it is impossible to block all inappropriate content. Where this is the case, we will raise the vigilance of colleague and learners through a learning programme and the embedding of E-safety in The Learning Foundry daily life.

4.3 As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build learners' understanding of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. They also need to be aware of the possible legal implications of their online activities.

4.4 Learner inductions:
All Learners who register and enrol with The Learning Foundry will undergo an E-safety specific induction which highlights the Do's and Don'ts of E-safety. This induction focuses on:

- Keeping personal data secure
- Use of social media whilst on site at The Learning Foundry
- Use of social media whilst placed with an employer
- Comments on social media

4.5 The Learning Foundry will:

- Put in place a continuous programme of awareness for both learners and colleagues
- Maintain E-Safety incident reports
- Ensure all colleagues know what to do in the event of an E-safety incident
- Record all incidents of E-safety
- Provide E-safety training as part of their induction programme for colleagues
- Provide training and advice for colleagues
- Regularly review training centres and meet with team members to discuss current issues, review incident logs and change control measures
- Report regularly to the Safeguarding lead on a quarterly basis
- Ensure relevant security is in place for the protection of the computer network
- Provide regular staff training on Safeguarding and Prevent
- Operate a register for consent to use personal data for the fulfilment of the learning contract which could include the production of videos and photographic material
- Ensure learners' full names will not be used anywhere on a website or blog, particularly in association with photographs

- Not publish learners' work without their permission and where appropriate their parents or carers permission
- Ensure visitors to site know that they should refrain from taking photographs without the permission of the safeguarding lead
- Make visitors aware that social media sites can be used when investigating complaints and potential disciplinary matters such as cyber bullying and harassment
- Ensure all colleagues have undergone E-safety awareness training

4.6 Colleagues will:

- Ensure they have an up to date awareness of E-safety and Social media usage matters and of the current E-safety policy and practices
- Report any suspected misuse or problem to the Safeguarding Lead for investigation
- Ensure any communication with learners is professional and only carried out using official systems
- Be aware of the risks of producing videos or photographic content
- Only use The Learning Foundry or Regenda owned equipment to produce video or photographic material
- Be aware of the consent required to produce videos or photographic content and use the Group content consent form
- E-safety issues are embedded into everyday learning
- Monitor ICT activity in sessions
- Pre-check all websites, videos and content that are to be used in learner sessions and not use this content if deemed to be inappropriate
- Be aware of their obligations under Safeguarding, Prevent, the Data Protection Act and GDPR

4.7 Learners will:

- Report any suspected misuse or problem to their Tutor, Assessor or the Safeguarding Lead for investigation.
- Be responsible for only using the ICT systems including internet, email, digital video, mobile technologies etc for training purposes
- Not download or install software on The Learning Foundry equipment
- Only log on to The Learning Foundry learning platform with their username and password
- Operate a good understanding of research skills and the need to uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Know and understand policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand policies on the taking / use of images and on cyber-bullying
- Understand the importance of adopting good E-safety and social media usage, practice when using digital technologies out of The Learning Foundry offices

- Not take, use, share, publish or distribute images of others without their permission
- Not to use social media to make defamatory comments about their employers and their place of work
- Be aware of the risk of grooming by those with whom they make contact on the internet, through social media sites and on mobile devices
- Not partake in inappropriate communication/contact with others, including strangers
- Not incite or participate in cyber-bullying or discrimination
- Not access unsuitable video/internet games/films
- Be aware of plagiarism and copyright infringement including the illegal download of music and videos
- Refrain from sending offensive messages which with may offend or cause damage to persons or companies
- Not disclosing confidential/personal information including passwords

4.8 Learners, colleagues or anyone acting on behalf of The Learning Foundry will not visit internet sites, make, post, download, upload, transfer, communicate or comment on material that could cause offence or relate to sexual abuse images, promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation, adult material that potentially breaches the Obscene Publications Act in the UK, criminally racist material, pornography, promotion of any kind of discrimination, promotion of racial or religious hatred, threatening behaviour (including promotion of physical violence or mental harm), promotion of extremism.

4.9 Cyber bullying is bullying through the use of communication technology e.g. mobile phone text messages, social media sites, twitter, emails or websites. This can take many forms for example;

- Sending threatening or abusive text messages or emails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (e.g. Facebook, twitter, Instagram etc.) or online diary (blog)
- Making or sharing offensive or embarrassing videos or photographs of someone via mobile phone or email
- It should be noted that bullying including the use of ICT to bully is against The Learning Foundry's Equality and Diversity policy and could be against the law.
- Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the Harassment Act 1997 or the Telecommunications Act 1984
- Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the bullied emotionally and/or physically

- ‘Bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g. graffiti, text messaging, email or postings on websites. It can be done physically, financially (including damage to property) or through social isolation’

4.10 If a bullying incident directed at a learner occurs using email or mobile phone technology:

- Advise the learner not to respond to the message
- Report to Regenda ICT Team
- Secure and preserve any evidence
- Inform the sender’s email service provider
- Notify parents of the learner involved
- Inform the Safeguard lead (where necessary)

4.11 If malicious or threatening comments are posted on an Internet site about a learner or member of staff, you need to:

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to CEOP (Child Exploitation and Online Protection Centre part of NCA national Crime Agency)
- Endeavour to trace the origin and inform police as appropriate
- Inform Safeguard lead.

5. Associated documents

- The Learning Foundry Safeguarding Policy
- The Regenda Group Information Security and Systems Usage Policy
- Equality and Diversity Policy
- Data Protection Policy / GDPR
- Code of Conduct

6. Development and implementation

This policy has been developed through the requirements for the business to meet the Safeguarding standards and is identified as good practice within the education industry.

7. Equality, diversity and human rights

The Learning Foundry is committed to ensuring that no person or group of persons will be treated less favourably than another person or group of persons and will carry out our duty with positive regard for the following protected characteristics: age, disability, gender reassignment, marriage and civil partnerships, pregnancy and maternity, race, religion, sex, sexual orientation. We also recognise that some people experience disadvantage due to their socioeconomic circumstances, employment status, class, appearance, responsibility for dependants, unrelated criminal activities, being HIV positive or with AIDS, or any other matter which causes a person to be treated with injustice. The Learning Foundry will also ensure that all services and actions are delivered within the context of current Human Rights legislation.

8. Monitoring and reporting

Managing Director
The Managing Director is responsible for this policy.

Assessors/Tutors/ The Learning Foundry Colleagues
Assessors/Tutors/all The Learning Foundry colleagues are responsible for reporting any breach of safety to the ICT team and Safeguarding Lead, if appropriate.

Regenda ICT team
The Regenda Group's ICT team is responsible for carrying out a full investigation into the breach and providing a report for the Managing Director and Safeguarding Lead.

The Learning Foundry Management Team
All Safeguarding incidents will be reported into The Learning Foundry Management Team.

9. Risk management

9.1 This Policy has been developed to mitigate the following risks:

- Inadequate ICT infrastructure
- Failure of Safeguarding provisions