LIMM SKILLS ACADEMY LTD
Innovation | Creativity | Empowerment

LIMMS E-SAFETY POLICY

1. Introduction

Limms Skills Academy recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within Limms, and to support staff and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay 'e-safe' and to satisfy our wider duty of care. This e-safety policy should be read in conjunction with other relevant Limms policies procedures.

2. Definition of E-Safety

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection.
e-safety risks can be summarised under the following three headings.

2.1 Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films

2.2 Contact

- Grooming using communication technologies, potentially leading to sexual assault or child prostitution
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Bullying via websites, mobile phones or other forms of communication device

2.3 Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

3. Scope

The policy applies to all persons who have access to Limms IT systems, both on premises and remote access. Any user of Limms IT systems must adhere to e-Safety Rules. The E-Safety Policy applies to all use of the internet, and electronic communication devices such as e- mail, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information.

4. Aims

The aims are to:

4.1 To ensure safeguards on Limms IT-based systems are strong and reliable

4.2 To ensure user behaviour is safe and appropriate

4.3 To assure that the storage and use of images and personal information on Limms IT- based systems is secure and meets all legal requirements

4.4 To educate Staff and learners in e-safety

4.5 To ensure any incidents which threaten e-safety are managed appropriately

5. Outcomes

5.1 Security

Limms networks are safe and secure, with appropriate and up-to-date security measures and software in place.

5.2 Risk assessment

When making use of new technologies and online platforms, staff are to assess the potential risks that they and their learners could be exposed to.

5.3 Behaviour

- It is an unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person. This also applies to use of social media systems accessed from Limms systems.

- All users of technology adhere to the standards of behaviour set out in the IT Acceptable Use Policy.

- All users of IT adhere to Limms guidelines when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras, etc.

- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and student disciplinary procedures.

- Any conduct considered illegal is reported to the police. Staff must take responsibility for moderating any content posted online.

- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the Lead Safeguarding Manager.

- Staff should keep personal and professionallives separate online

- Staff should not have students as 'friends' on social media sites that share personal information.

- Staff should be wary of divulging personal details online and are advised to look into privacy settings on sites to control what information is publicly accessible.

- Staff should recognise that they are legally liable for anything they post online.

- Staff are expected to adhere to the Limms' equality and diversity policy at all times and not post derogatory, offensive or prejudiced comments online.

- Staff should not bully or abuse colleagues/students online.

- Staff entering into a debate with a student online should ensure that their comments reflect a professional approach.

- Staff should not post any comments online that may bring Limms into disrepute or that may damage the college's reputation.

- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of Limms views, even with a disclaimer, and should consider their postings carefully.

- Staff should not use their Limms e-mail address to join sites for personal reasons or make their Limms e-mail address their primary contact method.

- Staff should be aware that any reports of them undertaking inappropriate online activity that links them to the Limms will be investigated and may result in disciplinary action.

5.4 Use of images and video

- The use of images or photographs is encouraged in teaching and learning. Providing there is no breach of copyright or other rights of another person.

- Staff and learners are trained in the risks in downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example.

- Limms staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe.

- Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any materials.

5.5 Personal information

- Processing of personal information is done in compliance with the Data Protection Act 1998.
- Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
- No personal information is posted to the Limms website/intranets without the permission of a senior manager.
- Staff keep learners' personal information safe and secure at all times.
- When using an online platform, all personal information is password protected.
- No personal information of individuals is taken offsite unless the member of staff has the permission of their manager.
- Every user of IT facilities logs off on completion of any activity, or ensures rooms are locked if unsupervised, where they are physically absent from a device.
- Limms mobile devices that store sensitive information are encrypted and password protected.
- Personal data no longer required, is securely deleted.

5.6 Education and Training

- Staff and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.
- Learner inductions and the tutorial programme contains sessions on e-safety.

- Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.

- Learners know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of

a random search.

- In classes, learners are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

- Any new or temporary users receive training on the Limms IT system, they are also asked to read, agree and sign an Acceptable Use Policy.

6. Incidents and response

- A clear and effective incident reporting procedure is maintained and communicated to learners and staff.

- Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.
- Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected learners, etc.

7. Responsibilities

- The Head of IT Services and Lead Safeguarding Manager are responsible for maintaining this policy, and for maintaining best practice in IT procedures and practices to manage any e-safety risks effectively.

- The following are responsible for implementing it:-

  - The Director of Human Resources for all e-safety matters in relation to Limms Staff.

  - Lead Safeguarding Manager for all e-safety matters in relation to Limms Learners.

  - The Head of IT Services for championing good e-safety practice in Limms IT facilities and processes, and for providing technical expertise when issues are being investigated.

  - Learning Development Coach Coordinators and Advanced Learning Officers for providing pastoral and practical support for learners dealing with issues related to e-safety and for

incorporating e-safety in student induction, supporting the tutorial scheme of work, and for providing an appropriate range of resources to tutors.

- All tutors for embedding e-safety education and practice into their teaching programme.

- All Limms Managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.

- All members of Limms staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

8. Access to the Policy

The policy will be published on the Intranet under 'Safeguarding'.

9. Monitoring and Review

The impact of the policy will be monitored regularly with a full review being carried out at least once every year. The policy will also be reviewed where concerns are raised by the Safeguarding Manager, or where an e-safety incident has been recorded.

10. Legal and other Frameworks

- Racial & Religious Hatred Act 2006
- Sexual Offences Act 2003
- Police & Justice Act 2006
- Computer Misuse Act 1990 (s1-3)
- Communications Act 2003 (s127)
- Data Protection Act 1998
- Malicious Communications Act 1988 (s1)
- Copyright, Design & Patents Act 1988
- Public Order Act 1986 (s17-29)
- Protection of Children Act 1978 (s1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulatory of Investigatory Powers Act 2000
- Prevent Duty Guidance: for Further Education institutes in England and Wales

I have read and understood E-Safety Policy.

Signature: _____

Print name: _____.

Date: _____