LESLIE FRANCES
HAIRDRESSING TRAINING

E-SAFETY POLICY

This Policy is linked to
- Safeguarding Policy
- Anti-Bullying Policy
- Anti-Cyber bullying Policy
- "Prevent Duty" Risk Assessment

Leslie Frances is committed to providing a safe and secure environment for learners, staff and visitors and promoting a climate where learners and staff will feel confident about sharing any concerns which they may have as a result of online safety issues. We recognise the need to be alert to the risks posed by strangers or others, extremism and radicalisation and those who may wish to harm.

We will take all reasonable steps to lessen such risks by promotion of e-safety policy that are clearly understood and respected by all. The policy is applicable to all on and off-site activities undertaken by learners whilst they are the responsibility of Leslie Frances

Purposes
- To outline the nature of e-safety and how staff and learners may identify it.
- To identify simple ways in which e-safety issues can be reported to responsible adults.
- To provide a clear policy and guidelines to enable e-safety to be tackled effectively.

Guidelines

Why the Internet and digital communications are important
- The Internet is an essential element in 21st century life for education, business and social interaction. Leslie Frances has a duty to provide learners with high-quality Internet access as part of their learning experience.
- Internet use is a necessary learning tool for staff and learners. Internet use will enhance and extend learning
- Staff will be made aware of, and learners will be educated in, the safe use of the internet
- Clear boundaries will be set and discussed with staff and learners, for the appropriate use of the Internet and digital communications.
- Leslie Frances will ensure that the use of Internet derived materials by staff and by learners complies with copyright law

Information system security
- The ICT system security will be reviewed regularly by our external computer support company
- Virus protection will be installed and updated regularly.

E-mail

• Learners and staff should only use approved curriculum e-mail accounts and when working on training school business.

• Learners will be made aware of how they can report abuse and who they should report abuse to.

• Learners must report if they receive offensive or inappropriate e-mail.

• In e-mail communication, learners must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

• Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and Leslie Frances web site

• Staff or learner personal contact information will not be published.

• Leslie Frances Directors/Training Manager will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing Learners' images and work

• Photographs that include learners will be selected carefully so that images of individual learners cannot be misused.

• Permission, from parents or carers will be obtained before photographs of learners are published on Leslie Frances Web site

• Work can only be published with the permission of the learner.

• When using digital images, staff should inform and learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Learners must not take, use, share, publish or distribute images of others without their permission.

Social networking and personal publishing

• Leslie Frances will educate people in the safe use of social networking sites. Learners will be advised to make their profiles private and secure as possible. They are taught to consider the appropriate and safe times when they can give out personal details which may identify them, their friends or their location.

• Learners must be made aware of how they can report abuse and who they should report abuse to

• Learners should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.

• Learners should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Learners should only invite known friends and deny access to others.

• Learners will be taught about being resilient to radicalisation, with an awareness made to the different ways that this may occur, including grooming. (See Prevent Duty in Safeguarding Policy)

Managing monitoring and filtering

• If staff or Learners discover an unsuitable site, it must be reported to the Training Manager)

• Our external computer support company will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

• Terminology related to specific forms of radicalisation will be added to the school filtering system in order to protect learners.

• All staff will follow the schools safeguarding procedures if any changed behaviour is observed.

Managing emerging technologies

• Emerging technologies will be examined for educational benefit before use in school is allowed.

• Leslie Frances is aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

• Where contact with learners is required to facilitate their safety (e.g. on trips), staff will be issued with a school phone.

• The sending of abusive or inappropriate text messages is forbidden.

Managing Social Media both Private and for Official Leslie Frances use

• This applies to social networking sites (for example Facebook, Instagram, SnapChat), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, and content sharing sites such as flickr and YouTube.

• Users should be conscious at all times of the need to keep their personal and professional/training school lives separate. They should not put themselves in a position where there is a conflict between the training school and their personal interests;

• Users should not engage in activities involving social media which might bring Leslie Frances into disrepute;

• Users should not represent their personal views as those of Leslie Frances' on any social medium;

• Users should not use social media and the internet in any way to attack, insult, abuse or defame learners, their family members, colleagues, other professionals, other organisations or Leslie Frances

Personal use of Social Media

• Learners should not have contact through any personal social medium with any member of staff, other than those mediums approved by the Senior Management Team, unless the staff concerned are family members. This stipulation remains extant for two years after the learner has left Leslie Frances.

• Photographs, videos or any other types of image of learners and their families or images depicting staff members, clothing with Leslie Frances logos or images identifying Leslie Frances' premises should not be published on personal unprivate or public web space without prior permission from Leslie Frances

• All staff and learners are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. All staff and learners should keep their passwords confidential, change them often and be careful about what is posted online

• We accept that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. Linkedin. We advise that care is taken to maintain an up to date profile and a high level of presentation on such sites if Leslie Frances is listed

Using Social Media –

• Leslie Frances Senior Management Team have full responsibility for running Leslie Frances' official website, Facebook, and Twitter sites.

• Staff wanting to set up department Facebook or Twitter feeds must have permission from the Senior Management Team and be followed accordingly

• Whilst learners are encouraged to interact with these social media sites they should do so with responsibility and respect. Protecting personal data

• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Authorising access
• All staff must read and sign the E-Safety Policy' before using any school ICT resource, including an iPad issued for professional use.
• Leslie Frances will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to Leslie Frances network. Leslie Frances cannot accept liability for any material accessed, or any consequences of Internet access.
• Leslie Frances will annually audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. Leslie Frances will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken
• Any complaint about staff misuse must be referred to the Training Manager and if the misuse is by the Training Manager it must be referred to the Directors in line with the School Safeguarding and Child Protection procedures.
• Learners and staff will be informed of the complaints procedure.

Communicating E-Safety

Introducing the E-Safety Policy to learners

• E-safety rules will be posted in all rooms where computers are regularly used. All system users will be informed that network and Internet use will be monitored.
• A programme of e-safety training and awareness raising will occur during theory lessons and reviews.

Staff and the E-Safety policy

• All staff will be given access to the E-Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops and iPads.
• Staff that manage filtering systems or monitor ICT use will be supervised by Senior Management Team to ensure clear procedures for reporting issues.
• Staff should understand that phone or online communications with learners can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Reporting e-safety breaches

• It is hoped that all members of Leslie Frances will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse.
• No definition of 'indecent' material has been written in law and it is up to interpretation by a jury. As guidance: Unsuitable material-Any information or images that can cause upset to a child;

• Pornography • Swearing • Violence/ cruelty • Bullying • Gambling • Sites which encourage vandalism, crime, terrorism, eating disorders, suicide. • Unmoderated chat Illegal material Anything illegal in the real world is illegal in the digital world; • Child exploitation • Child abuse • Grooming • Extreme violence • Racist Material . radicalisation

Monitoring

• The Training Manager will ensure that full records are kept of incidents.

• These records will be reviewed termly by the Training Manager and Safeguarding Co-ordinators. The Training Manager and Directors will review them when a serious incident occurs. Enlisting parents' and carers' support

• Parents' and carers' attention will be drawn to the e-safety Policy on Leslie Frances website