Use of Computers, Mobile Phones, Confidentiality, the Internet, and Social Utility Sites Policy

Introduction: The Leicester Tigers Foundation is committed to safeguarding the privacy and dignity of young people while ensuring that information is handled confidentially. This policy outlines the acceptable use of computers, mobile phones, and the internet, including guidelines for social utility sites. Our aim is to protect both the Foundation and the young people in our care, while upholding our commitment to safeguarding.

Role of the Designated Safeguarding Lead (DSL): The DSL is responsible for:

- Overseeing the implementation and adherence to this policy.
- Providing guidance and support on safeguarding issues related to ICT and mobile phone use.
- Reviewing and updating the policy in accordance with changes in legislation and best practices.
- Addressing any concerns or incidents related to ICT use and safeguarding.

What We Do:

1. **Computer Use:**
    - **Security Measures:** Users must take appropriate measures to prevent unauthorized access by enabling the security features available on the computer.
    - **Screen Privacy:** Enable the screen saver to blank the screen at regular intervals, ensuring that sensitive or confidential material is not left visible.
    - **Information Management:** Delete information once it has been printed if it is not required to be kept in dedicated files on the computer.
    - **Visibility:** Ensure the computer screen is not easily visible to visitors.
2. **Social Networking Sites:**
    - **During Working Hours:** Employees must not access social networking sites during contact time with young people or during working hours.
    - **Out of Work Hours:** Employees should not disclose any information about their place of employment on personal social networking profiles. This includes avoiding mention of work-related matters, names of staff, or young people.
    - **Supervision:** Young people should not be encouraged to access social networking sites. If a young person visits such a site, it should be recorded in their daily log, and they must be supervised if allowed to use such sites.

- **Contact Restrictions:** Employees must not accept or initiate contact with young people through social networking sites or email. Any such attempts must be reported to the line manager.

3. **Mobile Phones:**
   - **Classroom Environment:** Mobile phones are only to be used for study purposes in the classroom environment. Relevant websites can be accessed via the secure 'Education' wifi.
   - **Disciplinary Action:** Failure to adhere to this policy may result in disciplinary action or a ban on mobile phone use during classroom time.
4. **Filtering and Monitoring:**
   - **Responsibilities:** The Foundation is committed to filtering and monitoring online activity to safeguard young people. All staff will receive training on these processes.
   - **Monitoring System:** Day-to-day monitoring and managing will be overseen by the ICT, Pastoral, and External systems (Securus). Staff will remind young people of the filtering and monitoring systems periodically.
   - **System Review:** The Foundation's filtering and monitoring system will block harmful and inappropriate content while supporting teaching and learning. The AI data system will be reviewed periodically to ensure it remains fit for purpose.

Four Cs of Online Safety:

- **Content:** Ensure that all content accessed and shared via ICT equipment is appropriate and does not expose young people to harmful material. This includes implementing and maintaining filtering systems to block inappropriate content.
- **Contact:** Online communication with young people should be conducted through approved channels only. Staff should protect their personal contact information and maintain professional boundaries.
- **Conduct:** Staff should model appropriate online behavior, adhering to the Foundation's Code of Conduct. All interactions with young people should be transparent and respectful.
- **Commerce:** Staff should exercise caution regarding online commercial activities. Ensure that any transactions involving young people are secure and follow the Foundation's financial policies.

Storage and Confidentiality:

- **Information Security:** All information stored on computers must be handled in accordance with the Foundation's Data Protection Policy. This includes ensuring that personal data is securely stored and confidentiality is maintained.
- **Breaches:** Any breaches of data protection or confidentiality should be reported to the DSL and addressed promptly.

Policy reviewed in Sep 24. Next review Sep 25