RODOLFUS CHORAL FOUNDATION

The Rodolfus Choral Foundation Limited

DIGITAL & E-SAFETY – ACCEPTABLE USE (for Staff)

Reviewed: ***May 2025***

Next Review: ***May 2027***

Author: ***Annabel Price (Designated Safeguarding Lead)***

Approved: ***Binath Philomin (on behalf of the Board of Trustees)***

KEY TERMINOLOGY

The Foundation refers to **The Rodolfus Choral Foundation**

The OT refers to **The Operations Team**. This would usually comprise the General Manager, Course Operations Manager, Communications Manager, Access and Partnerships Manager and the Choir Team.

Adult refers to all people 18 and over. This includes staff, volunteers, observers and guests.

Staff refers to all those who work for or on behalf of The Foundation in any capacity whether paid or voluntary. All staff working for the foundation will be over the age of 18.

Parent refers to birth parents or other adults who are in a parenting role e.g guardians, stepparents or adoptive parents.

Young person/Student (here) refers to all people who may be participants in The Foundation's courses and choirs (excl. Adult Courses). This includes participants on Senior Courses or singers in the Rodolfus Choir who may be aged between 18 and 23.

DSL refers to the **Designated Safeguarding Lead**

ToS refers to the **Trustee with oversight of Safeguarding**

CoBT refers to the **Chair of the Board of Trustees**

1 PHILOSOPHY & CULTURE

The safety of young people on the Foundation's courses is paramount. In the new age of technology, digital devices and social media bring with them powerful opportunities in communication and teamwork but can equally pose several issues for children and young people with regards to personal safety and wellbeing when used inappropriately.

It is important to understand and recognise when this happens and how to act accordingly. The following guidance for STAFF is in addition to two crucial documents which can be found on the Foundation's website:

- **Safeguarding and Child Protection Policy; and**
- **Digital Strategy Policy**

This document aims to safeguard and protect students and staff when using digital communications, technology and social media.

2 CORE PRINCIPLES (Social Media)

Technology is a constantly changing medium and no policy can cover every social media site or application in full. It is advised therefore that you follow these key principles when dealing with any and all sites and applications:

- Staff must not use social media to look up the accounts of, contact or interact with young people;
- Staff must not identify young people on social media by tagging or naming them;
- Staff must not respond to attempts to contact them on social media by young people, and any contacts made must be reported to the DSL or ToS and recorded;
- Staff must not use social media in a way that could bring the Rodolfus Foundation into disrepute;
- Where possible, all personal social media accounts should be set to 'private' so as not to be accessed by members.

For more information on the use of specific Social Media sites, please read Appendix A of this document.

3 DIGITAL COMMUNICATIONS (E-mail)

All email contact with students should go through The OT (Rodolfus Office). They can be contacted at the following email address:

- **charlotte@therodolfusfoundation.org.uk**

Staff are reminded of their obligations to:

- Direct members to contact the office with any queries.
- Contact the office if they need to get in touch with a student.

Staff are reminded that they should not:

- Obtain or attempt to obtain students' contact details (email address or otherwise)
- Give out their own contact details or those of other staff members

4 TECHNOLOGY & DEVICES

Staff should aim to model best practice and minimise device usage when in the presence of students.

Staff should actively encourage students who are glued to devices to engage and interact with their peers.

Staff should not use personal devices to take photos and videos of members, with the following exceptions:

- Mass shots/videos taken on concert day in the performance space with no individual identifiable clearly.
- Pre-approved use of personal devices for professional use by the Board of Trustees. The Social Media Manager on each course will be granted this permission, and, as per their signed contract, is expected to delete all pictures and videos after they have been uploaded at the end of a course.

Staff may need to use devices to communicate regarding logistics with other staff where appropriate.

Senior Staff will need regular access to their mobile devices for the purpose of communication with parents and for urgent safeguarding concerns.

Staff should be aware that they will be subject to the host venue's IT monitoring and filtering system. The information that the school/venue may monitor includes the addresses of websites visited, and the timing and duration of visits to websites. The Foundation will be informed of any inappropriate use of the Wi-Fi provided by the school/venue IT departments and will investigate and determine the disciplinary outcome for the individual involved.

5 TEACHING ONLINE

Should a member of staff wish to work with a student in another capacity (for instance to tutor privately, engage them in another musical activity) a discussion should take place with the DSL before initial contact is made (via the office).

More information on the Teaching Online can be found on the website in the Foundation's Digital Strategy Policy. Some key points below:

i. All online teaching, whether vocal/instrumental coaching or rehearsal sessions, should take place only with written permission from the General Manager.

ii. Dress code for staff and students must remain professional

iii. Staff should ensure they employ a non-descript backdrop when using video.

iv. All safeguarding responsibilities for staff remain and they should make any concerns known immediately to the DSL. Inappropriate or indecent behaviour from staff and/or students will result in serious action.

Appendix A Social Media Specifics

1. Facebook

Staff must ensure that their personal Facebook privacy settings are appropriate. If they have a professional page or account then the posts may be public, so staff should be aware that young people will be able to see these and that they must ensure that the content is therefore appropriate.

Personal accounts should be used with a constant reminder that young people can and will try to find out about staff members using their social media accounts. Staff accounts should be secure, and information shared privately.

Staff should never:

- Contact young people using Facebook (either publicly or privately).
- Send or accept friend requests from young people who are students of the Foundation.
- Post images, video, media or comments identifying individual young people.
- Interact with a young person's Facebook account (e.g. likes, shares, comments).

Staff may:

- Share and interact with all posts from the official Foundation account.
- Post about courses generally, never mentioning individuals and ensuring that the content is both appropriate and positive.
- Post and share 'mass' / 'group' shots and videos taken on concert day or in the studio, mass and group shots should feature no clearly identifiable individuals. Videos should not be taken by staff.

2. Twitter/X

Young people may well follow staff on Twitter/X, particularly as many staff use Twitter/X for professional purposes. If staff have a Twitter account, then it is advised that they ensure that young people cannot access it by selecting the option to 'protect my tweets'. Staff must make sure that any public content is appropriate.

Staff should never:

- Use Twitter/X to contact young people (either via a public tweet/post or direct message).
- Follow young people on Twitter/X.
- Post images, video, media or comments on Twitter/X identifying individual young people.
- Interact with a young person's Twitter account (e.g. favourites, shares, replies).

Staff may:

- Interact with the official Foundation Twitter/X account (favourites, shares, replies).
- Tweet and retweet 'mass' / 'group' shots and videos taken on concert day or recording day in the auditorium or studio, mass and group shots should feature no clearly identifiable individuals. Videos should not be taken by staff.
- Tweet generally about courses making use of Foundation handles and hashtags, never mentioning individual young people.

3. Instagram

Staff with Instagram accounts should ensure that their accounts are only visible to followers by turning on the 'Private Account' option within their Instagram profile settings. Staff must 'ignore' any follow requests to their Instagram account made by young people and in the case of business accounts staff must decline/ignore any interaction from young people.

Staff should never:

- Use Instagram to contact young people (publicly or privately).
- Follow young people on Instagram.
- Post images, video, media or comments on Instagram identifying individual young people.
- Interact with a young person's Instagram account (e.g. likes, sends, comments).

Staff may:

- Interact with the official Foundation Instagram account (likes, sends, comments);
- Post and share 'mass' / 'group' shots and videos taken on concert day or recording day in the auditorium or studio, mass and group shots should feature no clearly identifiable individuals. Videos should not be taken by staff.
- Post generally about courses making use of Foundation handles and hashtags, never identifying individual young people

4. TikTok

Staff should not post personal TikToks of their time on the course, unless they include no images/videos of young people.

5. BeReal

Staff should be aware of their surroundings when taking personal pictures on BeReal, no young people should be present.

6. Snapchat

Same as above and location services should be turned off at all times. The Foundation does not have and does not currently plan to open a snapchat account.

7. Other

All other social media sites or applications, including social/networking applications such as WhatsApp, should be used in accordance with the Philosophy, Culture and Core Principles stated at the head of this document.

Dating apps must be disabled while on courses and set to ghost, private or undetectable as appropriate to the site.