

Green Room Place (GRP) Digital & e-Safety Policy

Updated & Approved by Company Directors and Qualified Pastoral Staff on January 27th, 2025.

1. Purpose and Scope

Green Room Place (GRP) is committed to promoting a safe and secure digital environment for all students, staff, and visitors, in line with our safeguarding responsibilities. This Digital and E-Safety Policy outlines the measures in place to ensure the safety and well-being of students attending our residential and day courses, particularly in relation to their use of digital technologies. The policy applies to all online activities conducted during our programmes, including during residential stays, lessons, workshops, and online communications related to our services.

This policy is designed to comply with UK laws and guidelines, including:

- **The Data Protection Act 2018**
- **The Children Act 1989 and 2004**
- **The Education Act 2002**
- **Keeping Children Safe in Education (2023)**
- **The Protection of Children Act 1999**
- **The Counter-Terrorism and Security Act 2015 (Prevent Duty)**

It applies to all students aged 10-20 who attend GRP's music courses, including both residential and day courses, and covers all team members, including directors, teaching staff, and pastoral team members.

2. Policy Aims

This policy aims to:

- Ensure the safety of students when using digital devices, online platforms, and the internet during GRP programmes.
- Provide a framework for the responsible use of digital technology by both students and staff.
- Educate students on the importance of e-safety, including the risks associated with digital technologies, cyberbullying, and privacy protection.
- Outline the procedures for reporting any e-safety concerns or incidents.
- Ensure compliance with the **Data Protection Act 2018** and relevant safeguarding legislation.

3. Roles and Responsibilities

- **Team Members:** All GRP staff and team members, including teaching staff, pastoral staff, and directors, have a responsibility to ensure that students are safe and secure when using digital devices and online platforms. Staff must be familiar with this policy and ensure its implementation, providing guidance on safe and appropriate use of digital technology. They must also ensure compliance with safeguarding guidelines and report any concerns in line with **Keeping Children Safe in Education (2023)**.
- **Students:** All students are expected to follow this policy, use technology responsibly, and report any concerns to a member of staff or the Nominated Child Protection Officer (NCPO).
- **Parents/Guardians:** Parents and guardians of students under the age of 18 are encouraged to discuss e-safety with their children and reinforce the importance of online safety both during and outside of the residential or course environment.

4. E-Safety Education and Awareness

As part of GRP's commitment to safeguarding, all students attending a residential course will be educated on e-safety during their orientation. This education is in accordance with **Keeping Children Safe in Education (2023)** and is designed to ensure that students understand the risks associated with digital technologies and how to stay safe online. Key topics covered will include:

- **Digital Footprints:** Understanding the long-term impact of online actions and the importance of protecting personal information.
- **Cyberbullying Prevention:** Identifying and addressing cyberbullying, as well as understanding the consequences of online harassment.
- **Safe Online Communication:** Guidelines for maintaining respectful and safe communication on digital platforms.
- **Privacy and Data Protection:** Basic principles of safeguarding personal data and privacy while online.

This education is delivered as part of the student orientation process at the beginning of each residential course, ensuring that students understand the importance of e-safety and are aware of the resources available to them if they encounter any issues. This aligns with **The Education Act 2002**, which mandates safeguarding and promoting the welfare of students.

5. Internet and Device Use

- **Internet Access:** Students are provided with internet access during their time at GRP residences and day courses. The internet is intended for educational and recreational purposes. While GRP will make reasonable efforts to ensure students' safety online, students are expected to use the internet responsibly, in accordance with UK laws, including **The Data Protection Act 2018**.
- **Acceptable Use of Technology:** Students must agree to use technology, including computers, phones, and tablets, responsibly and only for appropriate activities. This includes respecting copyright, refraining from accessing inappropriate content, and being mindful of others' privacy online.
- **Monitoring:** Internet use may be monitored during residential courses to ensure students are engaging in appropriate online activities. This monitoring will be in line with GRP's safeguarding responsibilities and will be proportional to the level of risk posed, in accordance with **The Data Protection Act 2018** and **Keeping Children Safe in Education (2023)**.
- **Mobile Phones:** Students will be informed of the mobile phone policies during orientation. For residential courses, mobile phones may be restricted in certain areas or times to ensure that students engage fully in the course activities and foster an environment conducive to learning and personal growth.

6. Social Media Use

- **Guidelines for Social Media:** Students are encouraged to use social media responsibly. They should be mindful of what they share online and consider the potential impact on their personal privacy and reputation. They should avoid posting anything that could be seen as inappropriate or harmful to themselves or others.
- **GRP Social Media Presence:** GRP may share updates about courses, performances, and other events on social media platforms. Students will be informed about the guidelines and permissions required before being included in any public-facing media or content shared by GRP.
- **Cyberbullying:** Students should report any incidents of cyberbullying to a member of staff immediately. All reports will be taken seriously and dealt with appropriately in line with GRP's safeguarding policies.

7. Online Communication and Behaviour

- **Respectful Communication:** All students and staff are expected to communicate respectfully and responsibly when using digital platforms. This includes using appropriate language, showing respect for others, and avoiding online behaviours that could be considered harassment, bullying, or discrimination.

- **Reporting Concerns:** If a student experiences or witnesses inappropriate online behaviour, they are encouraged to report it immediately to a member of staff, the NCPO, or via the GRP safeguarding procedure. All concerns will be dealt with promptly and confidentially, in accordance with **The Children Act 1989 and 2004** and **Keeping Children Safe in Education (2023)**.
- **Staff Interaction with Students:** Staff will adhere to professional standards when interacting with students online. All online communication between staff and students must be conducted in a manner that is respectful and within the boundaries of professional behaviour as outlined by **The Education Act 2002**.

8. Cybersecurity and Data Protection

- **Protection of Personal Information:** GRP is committed to safeguarding the personal data of all students, staff, and visitors in line with the **Data Protection Act 2018**. All digital systems, including email, databases, and online communication platforms, will be secured to ensure that personal information is protected.
- **Use of Third-Party Services:** Where GRP uses third-party services (e.g., for online learning platforms, communication tools, etc.), care will be taken to ensure that these services comply with data protection regulations and maintain high levels of cybersecurity, in line with the **General Data Protection Regulation (GDPR)**.
- **Password Security:** Students and staff are expected to use secure passwords for all digital platforms and are advised to change passwords regularly. Students should never share their passwords with others unless explicitly required for educational purposes.

9. Procedures for Reporting E-Safety Concerns

Any concerns related to e-safety, including cyberbullying, inappropriate online content, or digital threats, should be reported immediately to a member of staff or the NCPO. The following steps should be followed:

- **Report the Incident:** Report any concerns or incidents to the NCPO, or an alternative staff member if the NCPO is unavailable.
- **Document the Concern:** All concerns should be documented as accurately as possible, including dates, times, and any relevant details.
- **Investigation:** All concerns will be investigated promptly. GRP will work in partnership with parents, guardians, or external agencies if necessary, and ensure that students are supported through any investigation process.

10. Review of Policy

This policy will be reviewed annually to ensure it continues to meet the needs of GRP's students and staff, reflects the latest developments in digital technology, and complies with UK laws and guidelines, including those set out in **Keeping Children Safe in Education (2023)** and the **Data Protection Act 2018**.

11. Related Policies

This policy should be read in conjunction with the following GRP policies:

- Safeguarding & Child Protection Policy
- Equal Opportunities Policy
- Anti-Bullying Policy
- Whistleblowing Policy
- Data Protection Policy
- Missing Young Person's Policy

By ensuring that all students and staff are aware of and follow these guidelines, GRP is committed to providing a safe, supportive, and responsible digital environment for all participants.