# ReConnect

## Online Safety Policy

**ReConnect Online Safety Policy**

**1. Introduction**
ReConnect is committed to ensuring a safe online environment for all students, staff, and stakeholders. This Online Safety Policy outlines our approach to safeguarding against online risks, ensuring appropriate use of digital technologies, and promoting responsible online behaviour.

**2. Purpose**
The purpose of this policy is to protect students and staff from harmful online content, cyberbullying, and misuse of personal data, while promoting the positive use of digital tools for learning and communication.

**3. Scope**
This policy applies to all students, staff, parents, and visitors who access the internet or use digital devices within ReConnect premises, during learning activities, or when representing the organisation online.

## 4. Key Principles

### 4.1 Online Safety Education

ReConnect will provide online safety education through lessons, workshops, and special sessions on responsible online behaviour, digital privacy, and cyberbullying prevention.

### 4.2 Appropriate Use of Technology

Staff and students are expected to use the internet and digital devices responsibly, adhering to the following guidelines:

- Only access educational materials relevant to learning tasks.
- Use secure, school-authorised platforms for communication and sharing of work.
- Report any suspicious or harmful online activity to a designated safeguarding officer immediately.

### 4.3 Digital Well-being

We prioritise the mental health and well-being of our students in the digital world. Guidance and support will be provided to ensure that students manage screen time effectively and are aware of the impact of social media on mental health.

## 5. Online Safety Roles and Responsibilities

### 5.1 Safeguarding Officer

The Designated Safeguarding Officer (DSO) is responsible for monitoring online safety across ReConnect. They will:

- Provide advice and training to staff on online safety.
- Investigate and respond to incidents of online harm, bullying, or inappropriate content.
- Liaise with external authorities, where necessary, to handle serious breaches.

### 5.2 Teachers and Staff

Teachers and staff will model responsible use of digital technology and ensure students follow appropriate guidelines. They are expected to:

- Be aware of students' digital activity during sessions.
- Report any concerns or incidents to the DSO.
- Provide support for students encountering online difficulties.

**5.3 Students**
Students must adhere to the principles of responsible digital citizenship, including:

- Respecting others online and avoiding harmful behaviour such as cyberbullying.
- Protecting their personal information and not sharing passwords.
- Reporting any harmful or uncomfortable online experiences to staff.

**5.4 Parents and Guardians**
Parents will be informed about online safety risks and practices through newsletters, meetings, and workshops. They are encouraged to:

- Monitor their child's online activity.
- Support their child in following the rules set out by ReConnect.

## 6. Online Communication and Social Media

### 6.1 Student Communication

All online communication between students and staff must occur through approved platforms, such as school emails, learning platforms, or video conferencing tools (e.g., Microsoft Teams). Personal messaging apps must not be used.

### 6.2 Social Media Use

ReConnect 1-1 prohibits any form of online harassment or inappropriate communication on social media platforms. Students and staff must not engage in any online activity that could harm the reputation of ReConnect or its members.

## 7. Data Protection and Privacy

### 7.1 Handling Personal Data

ReConnect will comply with data protection regulations (GDPR) to ensure that students' personal data is handled safely and only used for educational purposes. Students and staff will be taught the importance of privacy and protecting personal information online.

### 7.2 Online Platforms

ReConnect will use secure, GDPR-compliant platforms for teaching, learning, and communication. All student data stored or shared on these platforms will be subject to strict privacy controls.

## 8. Managing Online Incidents

### 8.1 Reporting Incidents

Any online safety incident, such as cyberbullying, exposure to harmful content, or breaches of personal data, must be reported to the DSO immediately. The incident will be logged and addressed according to the severity, with appropriate disciplinary or safeguarding measures taken.

**8.2 Responding to Breaches**
In the event of a serious online safety breach (e.g., hacking, major cyberbullying incident), ReConnect will:

- Take immediate steps to contain the issue.
- Inform parents/guardians and other relevant parties.
- Contact the necessary authorities or cybersecurity services for further investigation.

## 9. Monitoring and Review

This Online Safety Policy will be reviewed annually or in response to significant changes in technology or legislation. Feedback from students, staff, and parents will be used to inform updates and improvements to the policy.

**Date of Approval: 10/7/24**

**Next Review Date: 10/7/25**