Online Safety Policy

This Policy was last reviewed and approved in April 2024. HRAS International is committed to reviewing this policy annually.

Version	Date	Change	Author
1.0	April 2024	New policy	ED

Table of Contents

Who our policy applies to

This policy and the procedures that it underpins applies to all staff, including senior managers, paid staff, board members, agency staff, students and anyone working on behalf of HRAS International.

Aims and Purpose of this policy

- To provide staff and volunteers with the overarching principles that guide our approach to online safety.
- To protect young people and vulnerable adults who receive HRAS International services and who make use of information technology (such as mobile phones and the Internet) as part of their involvement with us.
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

We recognise that:

- The online world provides everyone with many opportunities, however it can also present risks and challenges.
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
- We have responsibility to help keep children and young people safe online, whether or not they are using HRAS International's network and devices.
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to promote online safety by:

- Appointing an online safety coordinator(s).
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code.
- Supporting and encouraging the people using our services to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that user names, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and young people who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision, support and training for staff and volunteers about online safety.
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.
- Asking all staff and volunteers not to communicate with young people through personal social media platforms, e.g. not accepting them as friends on websites such as Facebook, or switching privacy settings on websites such as Twitter or Instagram so that follower requests can be declined.

We are committed to reviewing our policy, procedures and good practice annually.

ENDS.