

## Social Media Policy

This policy sets out Connect IOW CIO's policy on social networking

Social networking activities conducted online outside work, such as blogging, involvement in any social networking sites such as Facebook, Twitter, Instagram, Tik Tok and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image. In addition, Connect IOW CIO has a firm commitment to safeguarding all children and adults in all aspects of its work

This policy has been written to set out the key principles and code of conduct that we expect of all members of staff, parents and visitors with respect to their responsibilities in connection with the use of social networking sites

### **Key Principles**

Everyone at Connect IOW CIO has a responsibility to ensure that they protect the reputation of the Organisation, and to treat clients, family members, colleagues and members of the CIO with professionalism and respect

It is important to protect everyone at Connect IOW CIO from allegations and misinterpretations which can arise from the use of all social networking sites

Safeguarding all adults and children is paramount and is a key responsibility of all members of staff. It is essential that everyone at Connect IOW CIO considers this and acts responsibly if they are using social networking sites outside of the Organisation. Anyone working in the CIO either as a paid employee or volunteer must not communicate with children via social networking

It is also completely unacceptable to communicate on social media about the Service Users, families or any member of the CIO in or out of work on personally owned equipment

Individual written photo consent will be given to the Chief Executive Officer from parents or carers before a package of support can begin. It is the responsibility of each member to make themselves aware of each Service User and their family's preference on photography before working with them. Separate consent is to be given regarding each social media platform

Connect IOW CIO has its own social media pages on Facebook and Instagram, they are exclusively run and used by the Chief Executive Officer and are password protected on locked devices to ensure GDPR is upheld

It is each employee's responsibility to delete work related photos from their personal devices, keeping such photos is in breach of this policy and can result in disciplinary action.

Policy last review date: 17.10.2025