Reducing the risk of Doxxing: A mini guide for social workers

Introduction

The Scottish Association of Social Work (SASW) and the Social Workers Union (SWU) are jointly committed to supporting the safety, wellbeing, and professional integrity of social workers across Scotland. In recent years, social workers have increasingly been targeted through doxxing, which is the deliberate publication of personal information online without consent, often with the intention to intimidate, harass, or undermine confidence in professional practice.

Given the sensitive nature of social work, practitioners must take proactive steps to protect their digital footprint. This guidance outlines practical measures to reduce risk and ensure personal and professional safety online.

Managing Personal Information

Social workers should take care to limit the availability of personal information online. Avoid sharing details such as your full name, home address, personal phone numbers, family information, or identifiable workplace references on personal accounts. Review privacy settings on all social media platforms to ensure posts, photographs, and friend lists are restricted to trusted contacts.

Maintain a clear separation between personal and professional online identities. You can do this by not referencing employers, job titles, or professional roles on your personal accounts.

Professional Conduct Online

Social workers are expected to uphold the highest standards of professionalism, including in digital spaces. Please don't post any information about past or present work with service users or supported people, or work situations, even in anonymised form. This includes using AI platforms outside of work, such as ChatGPT. This aligns with the BASW Code of Ethics.

Avoid engaging in online disputes or discussions relating to professional decisions or contentious issues connected to your role. Be mindful that any content shared online may be captured, shared, or misinterpreted outside its original context.

Strengthening Your Digital Security

Robust digital security is essential for reducing vulnerability to online targeting. Use strong, unique passwords for all accounts and enable two-factor authentication wherever possible. Ensure devices, apps, and browsers are kept up to date to reduce security vulnerabilities.

Regularly 'Google' yourself, search your name online to identify publicly available information and request removal where appropriate or change your privacy settings if your own account information appears.

Responding to Doxxing or Online Harassment

If you believe you have been targeted:

- Report harmful or unauthorised content to the relevant platform immediately.
- Notify your employer as soon as possible and seek support through internal safeguarding, HR, or management processes.
- Keep detailed records of any incidents, including screenshots, URLs, dates, and any communications received.

Seek advice if you require professional support or guidance.

Understanding Your Rights

Malicious sharing of personal information may constitute harassment or breach data protection legislation.

You have the right to safety, privacy, and protection at work.
Employers have a duty of care to support staff experiencing online harassment or threats.

Seek support from your employer, professional association, or trade union if you believe your rights have been infringed.

Conclusion

Social workers carry out vital work in challenging circumstances. Protecting your digital presence is an important part of safeguarding your wellbeing and ensuring you can continue to practise safely and confidently.

SASW and SWU remain committed to advocating for your safety and supporting you in navigating online risks.

Additional Resources

Read the BASW Code of Ethics here

Read the BASW Social Media Policy here

If you would like to discuss any concerns, please reach out to us:

n.ireland@basw.co.uk
SWUinfo@swu-union.org.uk

January 2026
SASW The professional association for social work and social workers | SWU Social Workers Union