Vale of Glamorgan Council
MANAGEMENT OF VIOLENCE AT WORK PROCEDURES
Appendix 3
REVEALING PERSONAL INFORMATION

Criminals and others may seek to use the Internet and social media to identify personal information about members of staff with a view to embarrassing, discrediting, harassing, corrupting, or blackmailing them or their families.

Employees living in rural locations, in sensitive posts, with uncommon names, or in high profile posts are particularly vulnerable to such attempts.

It is recommended that employees who are identified as at risk:

- Remove personal details from the edited electoral roll
- Ensure telephone numbers are ex directory
- Opt all family members out of online commercial search facilities such as 192.com
- Ask 'Google maps' to remove pictures of their house, car or persons from their site there are various sites that will help you to do this here is one example 4 Steps to Remove Your House From Google Street View (aarp.org)
- Register to avoid unwanted telephone via Telephone Preference Service (tpsonline.org.uk)
- Register to avoid unwanted mail via MPS Online the mailing preference service
- Ensure privacy settings for social media are set to the highest level
- Do not register on social media using the council .gov e-mail address
- Are careful when accepting 'friends' to access their social media
- Are not associated with inappropriate material on 'friends' social media
- Are not associated with social media of criminals
- Are not associated with the social media of persons involved in serious organised crime
- Remember that online users may not be who they purport to be
- Ensure all computers and mobile devices have up to date security and anti virus software installed
- Use strong passwords and never share them
- Shred all paperwork containing personal details
- Contact the Police if they become subject of online abuse linked to their occupation, if a 'spoof social media account is established purporting to be used by them, or if their genuine social media account is 'cloned', 'hacked', or 'taken over'. Also inform the line manager and complete and INC1 incident report form

It is recommended that employees in enforcement or sensitive roles do not post any of the following information on the Internet or social media:

- Details of your employer
- Details of your post
- Images in a council uniform or with a council badge and lanyard on.
- Mobile telephone numbers
- Home addresses
- Personal e-mail addresses
- Family members' details
- Hobbies and places frequented
- Details of vehicles
- Images or details of colleagues without their consent

It is recommended that employees:

- Do not advertise work related social events on the internet of social media
- Use internal intranet for all work-related social notices, and
- Vary premises frequented for work related social events

This document is available in Welsh / Mae'r ddogfen hon ar gael yn Gymraeg .