Social networking guidance

Overview

This guidance sets out the guidelines to observe when accessing and using social networking sites (SNS) on behalf of the Home Office. It is in line with the Home Office Board's decision published on 23 January 2009 to allow access to SNS only where there is a legitimate business case.

Scope

This guidance is recommended for adoption across Home Office HQ, its agencies and non-departmental public bodies (NDPBs).

Guidance

1. Access

- Access to SNS is only granted once a business case has been approved by your director. You can download the procedure for on making a request for access from Related Links.
- The functionality of access to SNS within Home Office ICT systems is limited. Additional functionality (for example, to enable active participation in SNS rather than passive monitoring) is only available through standalone PCs, the cost of which must be carried by the relevant business unit.

2. Identify yourself

- Identify yourself by your commonly used name. Only use a pseudonym if absolutely necessary, for example where a site does not allow multiple users with the same name and all possible variants of the name are already in use.
- Identify yourself as a Home Office official, unless there are exceptional circumstances, such as a potential threat to personal security. This should include job title or role within the organisation where appropriate so that your area of interest and expertise is clear to those with whom you are communicating. Never give out personal details such as home address and phone numbers.
- Be aware that participation on SNS may attract media interest in you as an individual.

3. Participate

- The civil service code applies to your participation online as a civil servant or when discussing government business. You should participate in the same way as you would with other media or public forums such as speaking at conferences.
- Remember that participation will mean that any comments or contributions will be permanently available and open to being republished in other media. It is

very difficult to remove comments once posted, so think carefully before you contribute.
- Take care to stay within the law and be aware that libel, defamation, copyright and data protection laws apply.
- Never disclose information from protectively marked material that you may see as part of your work.
- Ensure that contributions are presented in a way that befits both the site in question and the professional reputation of the Home Office.
- When responding to questions posted on social networking sites be alert to any that are, or appear to be, from a media organisation. Contact the press office for advice on handling such queries.

4. Separate professional and personal identities

- It is possible that there are circumstances where you will be using the same social sites for business purposes which you also use in a personal capacity. Ensure that there is a clear separation between your professional profile and your personal profile in such cases.
- Make full use of the 'friend list' and privacy features available on many social media sites.
- Never use your Home Office identity for personal matters or your personal identity for departmental matters.

5. Risks

- Many of the risks in using SNS apply equally to professional as well as to personal use.
- Be aware of the risks posed by the aggregation of unclassified data when posting to SNS.
- Be aware of the risks posed by posting too much personal information on SNS.
- Review your 'friend list' to ensure individuals are genuine and not pretending to be someone else.
- You will need to manage the additional risks associated with your role in the Home Office with access to information potentially of interest to those who may seek to damage the department - its security, assets and information. These may be criminals, hostile organisations and hackers.

6. Core principles

- Be credible: be accurate, fair, thorough and transparent.
- Be consistent: encourage constructive criticism and deliberation; be cordial, honest and professional at all times.
- Be responsive: when you gain insight, share where appropriate.
- Be integrated: wherever possible, align online participation with other offline communications.
- Be a civil servant: remember that you are an ambassador for your organisation.
- Be secure.

7. Further resources

- Engaging through social media: a guide for civil servants published by the COI in 2009. Includes general principles and guidance for those working in the specialist fields of press and marketing.
- Participation online: guidance for civil servants published by Cabinet Office in June 2008. Sets out the core behaviours which civil servants should observe.
- Managing the risk from online social networking published by CESG June 2010.
- Civil service code - sets out the duties and responsibilities of all civil servants.