MEDIA SCREENING: USE OF THE INTERNET IN EMPLOYMENT DECISIONS

A GOOD PRACTICE GUIDE FOR EMPLOYERS

MARCH 2011

Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Media screening: an overview</td>
<td>5</td>
</tr>
<tr>
<td>Why conduct media checks?</td>
<td>8</td>
</tr>
<tr>
<td>Media screening and the law</td>
<td>10</td>
</tr>
<tr>
<td>Fundamental principles of media screening</td>
<td>13</td>
</tr>
<tr>
<td>Risks associated with media screening</td>
<td>16</td>
</tr>
<tr>
<td>When should media checks be conducted?</td>
<td>17</td>
</tr>
<tr>
<td>Who conducts media checks?</td>
<td>20</td>
</tr>
<tr>
<td>How to conduct media checks</td>
<td>22</td>
</tr>
<tr>
<td>What to ask</td>
<td>25</td>
</tr>
<tr>
<td>‘Adverse’ internet usage and presence</td>
<td>26</td>
</tr>
<tr>
<td>Encouraging safe and appropriate internet usage</td>
<td>35</td>
</tr>
<tr>
<td>Summary</td>
<td>36</td>
</tr>
<tr>
<td>Glossary of terms</td>
<td>39</td>
</tr>
<tr>
<td>Appendix: Further guidance on current internet usage</td>
<td>43</td>
</tr>
</tbody>
</table>
Introduction

Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country’s essential services, facilities and networks from terrorism and other threats.

The National Infrastructure

Nine different sectors form what is known as the national infrastructure. These provide the services which support everyday life:

- Communications
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Transport
- Water

CPNI provides security guidance, training and research from a physical, information and personnel security perspective. It aims specifically to reduce the vulnerabilities within these sectors, with particular emphasis on the most critical elements. Loss or disruption to any of these could cause severe economic or social consequences or even loss of life.

In addition to the nine sectors above, CPNI also provides similar advice to organisations engaged in planning and running the London 2012 Olympics.

The aim of this guidance

This document provides guidance to employers in the critical national infrastructure (CNI) on how to use the internet to inform their employment decisions; specifically the process of screening an individual’s online presence and usage through researching open source internet sites and by asking questions about this behaviour during the pre-employment screening process and as part of ongoing personnel security procedures.

For the purposes of this guidance the terms ‘media screening’ and ‘media checks’ are used to describe this process.

This document is not intended to replace an organisation’s existing media screening policy, but rather to provide information about good practice in this area.

In writing this guidance CPNI has consulted a range of bodies, including employers from the private sector, other government departments, law enforcement agencies, information specialists and legal experts.

CPNI recommends that organisations seek professional advice, especially on employment law, when implementing or amending their media screening policy and procedures.
This document should be read in conjunction with other guidance published by CPNI, in particular:

- ‘A Good Practice Guide on Pre-Employment Screening’
- CPNI > Security advice > Personnel
- ‘Managing the risk from online social networking’
Media screening: an overview

In order to help evaluate a job applicant’s suitability for a role and to assess their security awareness when using the internet, it is becoming increasingly common for organisations and businesses to consider an individual’s ‘online reputation’ as part of their pre-employment screening, vetting processes and ongoing personnel security procedures. This is considered particularly important when the organisation conducts work of a sensitive nature and the role itself may involve access to sensitive sites and/or sensitive material, has a specific type of responsibility and/or is considered high profile (for example a senior position within an organisation and/or one that is outward facing).

The term ‘online reputation’\(^1\) is used to define ‘the publicly held social evaluation of a person based on their online behaviour, what they post and what others (such as individuals, groups and web services) share about this person on the internet’.

In order to establish ‘online reputation’, human resources (HR) professionals, vetting officers and security managers may conduct research on open source internet sites. In addition, questions may be asked about internet usage and presence during vetting interviews and as part of ongoing personnel security procedures. This process is known as ‘media screening’, ‘online screening’ or conducting ‘media checks’.

Based on interviews with 275 recruiters and human resources professionals and 330 consumers interviewed in the UK, Germany, France and the US, a report\(^2\) into what extent online reputation has become a significant factor found that:

- 41% of employers in the UK have rejected candidates based on information they found online;
- fewer than 9% of consumers surveyed believe that information found online would have an impact on them getting a job.

This shows that employers consider ‘online reputation’ significant enough for it to influence their recruitment decisions and that prospective employees significantly underestimate the level of data mining that is conducted and the impact it can have on their recruitment.

As media screening is becoming a more popular tool in pre-employment screening and ongoing personnel security procedures, it is important that employers have an up to date and informed understanding of the nature of internet usage amongst the working population and ensure that the process of media screening is conducted in a way that is both legitimate and proportionate.

---

1 Microsoft report ‘Online reputation in a connected world’, Cross-tab, January 2010
2 Ibid
The internet and society

Thanks to its widespread usability and access, the internet has enabled entirely new forms of social interaction, activities and organising. Increasingly people are using technologies such as social networks, blogs and websites to create and share content with others around the world. This has specific implications for recruitment and ongoing personnel security procedures.

Users of social networking sites, such as Facebook, are able to add a wide variety of information to their personal pages sharing common interests and ‘connecting’ with others.

 Millions of people use blogs or message boards as a means of communication and sharing ideas. Internet ‘chat’, whether in the form of chat rooms or via instant messaging systems, allows an individual to stay in touch at any time, day or night. Messages can be exchanged more quickly and conveniently than via email. Additionally, files can be exchanged, photographs shared and voice and video contact made between group members. Microblogging site Twitter allows users to stream a description of their activities in ‘real time’ as soon as it happens.

Live and recorded audio and video streams can be broadcast online and webcams allow viewers to watch live, real-time images (e.g. traffic at a local roundabout) or to share live video streams of themselves with others. YouTube is the leading website for free streaming video, claiming that its users watch hundreds of millions and upload hundreds of thousands of videos each day.

Social and political collaboration is becoming more widespread as internet usage grows. For example, the use of social networking in the 2009 Iranian election protests or the ‘flash mob’ events organised via Facebook.

As it is the fastest way to spread information to a vast number of people simultaneously, the internet has become a large market for business. It has revolutionised shopping (e.g. a product may be ordered online one day and delivered the next or downloaded instantly) and has also facilitated personalised marketing - which allows a company to market a product to a specific person or group. Online communities such as MySpace and Facebook, where users advertise themselves and share interests and hobbies, are perfect platforms for online companies to conduct market research and to advertise their own products to those users.

Online leisure activities which have become increasingly popular include: multi-player gaming where users can engage in real time role-playing games; gambling with other online participants; virtual reality worlds; the use of online dating sites and viewing pornography.³

³ For further information, see Appendix.
Privacy and disclosure

Current trends in internet usage have, perhaps unsurprisingly, raised a number of concerns about privacy and disclosure. Many of the above mentioned services require users to share personal details in order to access them and users may often unwittingly disclose personal information simply by storing information or cross-referencing databases.

The Oxford Internet Institute survey (Dutton and Helsper, 2007) found that 70% of UK internet users agreed or strongly agreed with the statement “people who go on the internet put their privacy at risk”. However, there is also evidence to suggest that many of those who express concerns about online privacy also fail to observe safe practices when using the internet and readily reveal personal information when prompted to do so.

Some users appear happy to share very personal information, opinions and thoughts when there is no requirement to do so, without considering the public nature of the internet and the security risks attached to this behaviour. This has been called ‘bunny slipper syndrome.’

Media headlines about the risks of social networking sites or the number of young people who are addicted to the internet also heighten concerns about the safety of internet usage. This can help to create a heightened fear of the drawbacks associated with its use. When assessing the impact of the internet on society it is also important to remember the many benefits it provides and that many users interact with it positively and securely.

Implications for recruitment and ongoing personnel security

For those in recruitment, HR, security and vetting, current trends in internet usage create benefits and risks. On the one hand, media screening potentially provides the employer with useful background information about an individual that can be used to assess their suitability for a role and the security risk they may present. On the other hand, the internet allows the individual to share both personal and work related information with a world wide audience. This may in turn damage the security and the reputation of the organisation they work for.

---

4 The Oxford Internet Institute survey, Dutton and Helsper, 2007
6 Definition: when internet users in the comfort, privacy and apparent safety of their own homes volunteer more personal/sensitive/intimate information than they would in other circumstances.
Why conduct media checks?

Depending on the nature of the organisation and the role in question, media checks may be carried out in order to assess whether a prospective or current employee:

- may be a reputational risk to the organisation due to their use of the internet;
- may be a security risk to the organisation and its employees due to their personal use of the internet;
- has not revealed/or concealed certain information about themselves which may be detrimental to the organisation;
- could be vulnerable to coercion as a result of their internet activities or presence;
- is using the internet to bully or harass other members of staff.

Media screening may be considered particularly important if the role an individual has applied for or currently holds includes:

- access to sensitive sites/areas of the organisation;
- access to sensitive material;
- a specific type of responsibility;
- is considered high profile.

Organisations may also consider using media screening to:

- help verify identity;
- help paint a more detailed picture of an individual’s lifestyle choices in order to determine whether any of them may present a security risk;
- determine whether a candidate is honest and has integrity;
- either confirm or negate any suspicions of inappropriate behaviour;
- establish how security aware the individual is and what their attitude is to sharing personal information online;
- investigate whether they have an ulterior motive for making the application, e.g. they are a journalist, criminal or activist who seeks to infiltrate the organisation;
- assess whether they are engaging in any illegal activities online;
- check the authenticity of previous work addresses;
- check for any sign of bankruptcy (where roles involve access to money);
- corroborate information from other checks on the individual (such as criminal record checks) which have highlighted a concern (e.g. conviction);
• determine whether the candidate holds any attitudes that may conflict with the ethos of the organisation, e.g. the police specify that no-one who openly shares racist or sexist views online will be employed;

• depending on where the candidate may be posted and the nature of the role, to identity anything online that may be exploited by foreign intelligence services or other organisations.
Media screening and the law

There is no specific legal constraint regarding the searching of open source information online. Anything on the internet is by definition, publically accessible. It is up to the individual how much personal information they make publically available. By putting it in the public domain individuals are consenting to others viewing and interacting with it.

However, there are a number of legal provisions in place to ensure that when an employer conducts media checks on a prospective or current employee, they do not interfere unduly with the individual's right to privacy, disclose any information they may find in an inappropriate way or without due cause, or use information sourced from media checks in a discriminatory way.

There are also a number of principles that should be applied when conducting media checks. These are outlined in more detail in the chapter: ‘Fundamental principles of media screening’.

The Human Rights Act 1998 (HRA) – Article 8

Article 8 ensures that everyone has the right to respect for their private and family life, their home and correspondence.

This means that one has the right to live one’s own life with such personal privacy that is reasonable in a democratic society, while taking into account the rights and freedoms of others. It includes the freedom for the individual to choose how they look, how they dress, with whom they socialise, and their sexual identity. It also includes the right to have information about individuals, such as official records, photographs, letters, diaries and medical information, kept private and confidential. Unless there is a very good reason, public bodies should not collect or use such information. Article 8 also includes mention of:

- access to information about a person’s own identity;
- a person’s right to have and to express an identity;
- the protection of a person’s reputation.

Interference with an individual’s right to privacy must satisfy three criteria to comply with the requirements of Article 8 in that it must be:

- in accordance with the law;
- have a legitimate purpose;
- proportionate to what it seeks to achieve.

---

7 www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1
Prospective and existing employees may argue that viewing online data about them violates their right to respect for private life pursuant to the Human Rights Act. This, however, is likely to be difficult to prove, particularly in light of an Employment Appeal Tribunal decision where it was held that information an individual has made publicly available on the internet could not be reasonably considered to be part of their private life.\footnote{Pay v Lancashire Probation Service, Employment Appeals Tribunal, 29th October 2003}

**Data Protection Act 1998 (DPA)\footnote{www.ico.gov.uk/what_we_cover/data_protection.aspx}**

Employers must ensure that all information gathered about an individual’s internet usage and presence is handled and stored in a legitimate way.

The Data Protection Act stipulates that anyone who handles personal information – i.e. any information that relates to an individual who can be identified by that information – has to comply with a number of principles:

- Data may only be used for the specific purposes for which it was collected.
- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (e.g. the prevention or detection of crime). It is an offence for other parties to obtain personal data (about a prospective or current employee) from the employer without authorisation.
- Individuals have a right of access to the information held about them, subject to certain exceptions (e.g. as above).
- Personal information may be kept for no longer than is necessary and must be kept up to date.
- Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.
- Subject to some exceptions, all entities that process personal information must register with the Information Commissioner’s Office.
- Individuals have the right to have factually incorrect information corrected (note: this does not extend to matters of ‘opinion’).
The Employment Practices Code

The Employment Practices Code is designed to help employers comply with the Data Protection Act and to encourage them to adopt good practice. It does not impose new legal obligations.

It covers data protection issues relating to recruitment and selection, employment records, monitoring at work and dealing with information about workers' health.

Employment law

Employment law applies to both those who are job applicants and to current employees. Recruitment decisions should not be based on age, race, gender, sexual orientation, religious or philosophical belief or disability. If any 'adverse' information found online can be interpreted as being specific to any of these attributes, an employer may be accused of being discriminatory if they choose to use it as a reason for not employing someone.

How to deal with ‘adverse’ material found online is covered in more detail in the chapter: ‘Adverse internet usage and presence’

When implementing or amending a media screening policy, CPNI recommends that organisations seek professional advice, especially in the area of employment law.

The Equality Act (2010)

Employers also need to be aware of the Equality Act (2010) which came into effect in October 2010.

The main purpose of the Act is to codify the Acts and Regulations which form the basis of anti-discrimination law. These are, primarily, the Equal Pay Act 1970, the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995 and three statutory instruments protecting discrimination in employment on grounds of religion or belief, sexual orientation and age.

This legislation requires equal treatment in access to employment as well as private and public services, regardless of gender, race, disability, sexual orientation, belief and age. In the case of gender, there are special protections for pregnant women. In the case of disability, employers and service providers are duty-bound to make reasonable adjustments to their workplaces to overcome barriers experienced by disabled people.


Fundamental principles of media screening

It is advisable to apply the following six fundamental principles when conducting media screening:

1. Proportionality

It is neither proportionate nor necessary to conduct media checks on all individuals during recruitment or to conduct media checks on all members of staff currently in post.

The end must justify the means. The Information Commissioner’s Office warns against reliance on arbitrary checks on an individual's private life where it does not affect work activity. An employer must have legitimate grounds for collecting, using and storing any online personal data about a prospective or current employee.

Risk assessment

In order to assess the potential security and reputational risks associated with a specific job role, it is advised that each role is risk assessed.

This involves considering:

- what level of access the role gives to the organisation's assets e.g. information, materials, systems, buildings and people; and/or
- whether the role is high profile; and/or
- has a specific type of responsibility e.g. financial or working with vulnerable others.

For further information on risk assessment, see the CPNI guidance: Risk Assessment for Personnel Security: A Guide.

Once each role has been risk assessed the employer can then decide whether media checks need to be conducted during pre-employment screening and employment.

Before conducting media checks employers should also consider:

- whether they can find the background information they need about this person in any other way. For example, through other more standard screening checks, during an interview with the job applicant or from referees;
- how much and what kind of online information is required.

12 www.ico.gov.uk
2. **Necessity**

In the process of trawling the internet, the employer may gain sight of large amounts of personal information about an individual, much of which may not be relevant to the individual’s prospective or current role. The employer must not collect more personal information than they need to help with their employment decision.

It is a breach of data protection rules to collect personal information that is irrelevant or excessive.

3. **A sense of perspective**

It is important to remember that internet checks form only part of the screening process and do not provide the whole picture.

It is also important to remember why an employer is conducting media screening in the first place. It is to ensure that the organisation, its reputation and its assets remain secure, not in order to make a personal judgement about an individual’s lifestyle choices or private behaviours.

If an individual chooses to share detailed personal information about themselves online an employer needs to assess whether this information has the potential to place the organisation and/or the individual at risk (of coercion, blackmail or social engineering) and not judge the individual themselves on what they find.

A prospective or current employee who has high internet usage and low security awareness may pose an increased risk to the security and reputation of the organisation because of their lack of security awareness, rather than because they choose to use the internet frequently. They should be advised on ways to reduce their online presence and make their internet activities more secure. For more information on the risks associated specifically with online social networking sites such as Facebook, see the CPNI guidance: ‘Managing the risk from online social networking’.

4. **Transparency**

Employers should make it clear to prospective and current employees what checks they are going to do from the outset and why they need the information the checks may provide. Employers are advised to have a clear policy on their use of media checking in both pre- and post-employment screening. If employers intend to carry out ‘top-up checks’ or ‘continuous checking’ this should also be entirely clear to all employees at the outset of their employment.

If an employer has no justifiable reason for doing online checks, then they should not be doing them.
5. **Consistency of approach**

Although it might not be possible to ensure consistency of interpretation, the ways in which information is sought, handled, reported and stored should be the same for all individuals.

6. **Privacy**

- only online information which can be publically accessed should be researched;
- if any information on prospective and current employees’ internet usage and presence is recorded, it must be kept securely and only for as long as there is a clear need.

It is not appropriate to ask a prospective or current employee direct questions about their personal internet usage and presence unless:

- something ‘adverse’ has been found online and the employer needs further details about it from the individual in question;
- the employer wishes to raise awareness of online security issues and is discussing this with employees during induction or as part of an annual appraisal or security review;
- a vetting officer is conducting a developed vetting (DV) interview;\(^\text{13}\)
- the individual in question is under investigation;
- it relates to the role in question or the individual’s suitability to the role.

For further details about ‘adverse’ online presence and usage see the chapter ‘Adverse internet usage and presence’.

\(^\text{13}\) For more information on DV, see page 17
Risks associated with media screening

Using the internet as an investigative tool can be very helpful. However, it is not without risks, particularly in regard to the attribution and verification of online information.

When looking at open source internet sites it is important to consider the following:

- **Verification of identity** – ensure that information found online relates to the right person. Be aware that if an individual has a very common name or if they share their name with a celebrity an internet trawl will potentially produce hundreds or thousands of hits. Therefore, it may become increasingly difficult to identify them correctly online.

- **Impression management** – be aware that people may present themselves online in a way that they would like to be perceived by others and this is not necessarily who they really are or how they usually behave in other circumstances.

- **Third party views and opinions** – be cautious when reading online information that has been written about an individual by someone else. Can material that other people have posted online about someone else be trusted? Consider the reasons why a third party might choose to write something negative or critical, for example.

- **Personal opinion** – try to remain as neutral as possible when judging others’ online presence and usage. Always consider whether their online behaviour will impact on their ability to do their job or whether it is something that you, as an employer, personally feel is inappropriate?

- **Time constraints** – be aware that some general internet trawls may not produce anything useful or relevant because the search engine returns many pages of results and there is only time to check the first few pages.
When should media checks be conducted?

Pre-employment screening

It is important to ensure that media checks should only be conducted if the employer can demonstrate that they are relevant to the role in question, e.g. the role is high profile, has specific types of responsibility or will place the individual in a potentially vulnerable position.

When screening a prospective candidate, media checks are primarily undertaken during or after other pre-employment screening activities. They should be carried out at as late a stage as practicable in the recruitment process, as the CV, referees and other pre-employment screening checks should have provided the employer with most of the relevant personal information required.

Additional media checks may also be undertaken as a result of a concern arising from an application form or an interview.

For example:

- if specific views have been expressed during an interview (i.e. of a discriminatory nature) which the organisation feels may need to be explored further;
- if there is any indication of membership of a political party that holds extremist views e.g. the police will not employ someone who holds membership of the British National Party (BNP);
- if there are any gaps in essential information on the application form (such as dates of employment or references);
- if the interviewer feels genuinely uncomfortable about responses on an application form or during an interview.

Depending on the nature of the concern, additional checks could include conducting further media checks or talking directly to the individual. Please see the chapter ‘Adverse internet usage and presence’.

Developed vetting interviews

Some public and private sector posts require the post-holder to have developed vetting security clearance. This is because they are ‘likely to have long-term, frequent and uncontrolled access to highly sensitive information or assets’.14 As part of the developed vetting process the applicant is required to have a face-to-face vetting interview and to provide a number of referees who will also be interviewed.

Applicants and their referees will be asked a series of questions about internet presence and usage. Online media checks are usually conducted after the interview with the applicant has taken place to further explore responses given, but may also be carried out prior to meeting the applicant as initial background research.

**Media checks during employment**

Media checks on personal internet usage and presence conducted on current employees tend to be undertaken:

- if an organisation conducts ‘top-up’ checks as part of its personnel security practice and the employee is aware that their personal internet presence and usage is monitored at certain times during their employment with the organisation;

and/or when an employee:

- is moving to a post that requires developed vetting status;
- is having their current vetting status reviewed;
- has been promoted to a more high profile role or one with specific responsibilities;
- is under investigation.

**‘Top-up’ checks and ‘continuous screening’**

‘Top-up’ checks, as part of ongoing personnel security procedures, are becoming increasingly popular with employers and commercial screening companies. Top-up checks are a series of refresher checks that are run at specific points during employment. This does not mean that all background checks are re-made.

‘Continuous screening’ means making background checks, including media checks, on staff at any stage of their employment.

**Transparency**

If employers intend to conduct media checks on current employees at any point during their employment, they must inform employees from the outset that this is standard practice and is consistent with the company’s policy concerning monitoring employees’ internet use. Any ongoing media screening processes and procedures should be clearly outlined in company documents such as policy, terms and conditions and code of conduct.

There is a potential risk that if an employer frequently conducts checks of employees’ personal internet usage and presence, this could undermine the employer’s duty of trust and confidence which is owed to the employee.
If an employer decides to take disciplinary action based on what they have found online this could give rise to claims for constructive dismissal or unlawful discrimination. This is discussed in more detail in the chapter: ‘Adverse internet usage and/or presence’.
Who conducts media checks?

The level of resource used to undertake media checks will depend on how important the organisation perceives this activity to be. Workload, size of organisation and time constraints may restrict the amount of media checking done.

Media checks may be carried out during pre-employment screening, vetting and as part of ongoing personnel security procedures by in-house HR and/or vetting departments. They may also be outsourced to government vetting agencies or commercial screening companies.

Government vetting agencies

The bulk of developed vetting (including media checks in response to online reputation questions) is outsourced to government vetting agencies, with one or two exceptions. Most organisations that require this process also have their own small in-house vetting teams. After completing the process the government vetting agency will make a recommendation to the sponsoring department as to whether someone should be issued with developed vetting clearance or whether the clearance should be upgraded or refused. In-house vetting teams might then conduct further media checks to help them reach a final decision.

Commercial screening companies

The use of commercial screening agencies to carry out pre-employment checks is reasonably commonplace. Increasingly, such agencies are offering ‘media checks’ as part of this service. This will include internet trawls and ‘adverse’ media searches. These agencies do not offer legal advice on such activities or an interpretation or assessment of the information found about a particular individual – it is left up to the company to decide whether the information is ‘adverse’ or impacts on their decision to hire the individual.

Training

Currently, it is not common practice for organisations to provide specific training on how to conduct media checks. Often those with experience pass down the tricks of the trade to new colleagues. An organisation needs to decide whether more formalised training would be useful.

In addition to providing open source training, it may also be useful for employers to advise media screeners on how to assess and report on internet usage and presence, particularly in relation to anything that is deemed ‘adverse’. This helps ensure a consistency of approach.
Other useful ways of sharing information about media screening may include:

- having regular meetings to share good practice and up-to-date information about popular applications (such as Twitter);

- producing guidance notes on current trends in internet usage and useful examples of popular websites on topics such as dating and gambling;

- rather than training people in-house, some private sector organisations outsourcing media checks to commercial screening companies who are perceived to have the necessary skills and knowledge.
How to conduct media checks

Open source checks

Open source means online information that anyone can access. Therefore, any information that an individual has shared on an open source site can be legitimately accessed by any other internet user, including a prospective or current employer.

General internet trawl

In the first instance, employers may conduct a general internet trawl to find any mention of the individual in question. This could result in finding:

- mention of membership of a professional body, club or society;
- mention within news or other articles;
- images of the individual;
- mention of membership of social and business networking sites;
- articles, blogs or microblogs that the individual has written.

Checking specific websites

Additionally, if an employer is concerned about the nature of an internet site that the individual (or one of their referees has mentioned during a vetting interview) they may wish to visit the site in question.

Again, it must be stressed that:

- only open source internet sites should be viewed;
- and only if the employer can justify why they thought the site was of concern and may therefore make the organisation and/or the individual vulnerable.

Social networking sites

Social networking sites such as Facebook, MySpace and Bebo have privacy options that restrict access. In general, this means that it is only possible to view and interact with an individual’s full profile page if they have given permission to do so. Some individuals, who are less security aware, may not fully restrict access to their profile page, thereby allowing all other internet users to view their profile and friendship lists and presenting a security issue. The risks associated with an individual’s personal use of social networking sites is discussed in CPNI’s guidance: Managing the risks associated with social networking.

Although an employer may decide to try and view social networking sites as part of their internet trawl (this is currently permissible) this data should not be gained by deceit (i.e.
without consent) as this would breach the Data Protection Act, Human Rights Act and European legislation.

**Getting started: where to look**

When looking for information on the internet most people initially use a search engine such as Google or Yahoo. However, this can return thousands of ‘hits’, particularly if the individual in question has a common name or shares their name with a celebrity. In order to refine the search it is advisable to use ‘deep web’ sites such as Pipl first before using a site such as Google.

**Searching the ‘deep web’**

Since most personal profiles, public records and other people-related documents are stored in databases and not on static web pages, a lot of online information about people is invisible to a regular search engine.

The term ‘deep web’ refers to a vast repository of underlying internet content, such as documents in online databases which general purpose web crawlers cannot reach.

The following ‘deep web’ sites pool internet presence:

- 123people.com
- Pipl
- Zoominfo
- Wink.com

123people allows the user to search by different countries, collates email addresses, photos, microblogs and Facebook and LinkedIn pages.

Zoominfo collates information that relates to business presence of user as does LinkedIn which is used for networking, sharing CVs etc.

**Search engines**

Once ‘deep web’ site such as 123people.com have been checked, a site such as Google can then be used to double check information found on these sites or to search for something more vague and difficult to find.

Other popular search engines include Yahoo and Ask.

It is advisable to use the Advanced Search facility on Google or any other search engine (e.g. uk:search.yahoo.com). Alternatively, an appropriate abbreviation (e.g. nhs.uk) can be used instead of completing the advanced search boxes. Advanced search also allows the user to filter time span. It is also possible to increase or decrease the number of search results per page. ‘Ask.com’ also provides the ‘lots of answers’ service.
Metasearch engines

The following metasearch engines allow the user to check many other search engines:

- Dogpile
- Browsys

Dogpile, for example, searches Google, Yahoo, Bing and Ask Jeeves.

Browsys displays tabs for areas such as ‘images’ and ‘social’. Twitter, Ning and Facebook are then displayed.

News and articles

Many organisations check www.bbc.co.uk or www.timesonline.co.uk for news and articles. Sites such as news.google.co.uk and www.silobreaker.com can also be helpful for pooling articles. www.silobreaker.com also searches blogs.

Subscription sites

There are a number of useful subscription sites such as global.factiva.com. This is a worldwide news database that pools articles from national, international, regional and local newspapers and journals. Searching can be further defined by companies, certain subjects of interest, industry and region and subjects that are not of interest, such as obituaries, can be excluded. Another site is lexis-nexis.com – a large organisation with access to countless databases, both legal and news.

Media websites

www.holdthefrontpage.com is an example of a site where employers who have concerns that a prospective employee may be a journalist can search for evidence of their background.
**What to ask**

**Application forms**

It is standard practice to ask a prospective employee to provide details of their email address/es on most application forms. It is not appropriate to ask an applicant to provide further details of their personal internet usage and presence on a standard application form.

**Interviews**

During interviews with prospective or current employees it is not common practice for the HR practitioner or line manager to ask an individual direct questions about their personal internet usage and presence. This would be considered outside of the line manager's remit and an invasion of the personal privacy of the individual.

Questions on this topic are more usually discussed:

- if any material of concern has been found during pre-employment media screening and the employer seeks further detail and clarification;
- when a security manager is discussing issues relating to company reputation and online security, perhaps as part of the organisation's induction process;
- if it is practice for online security issues to be discussed during an annual appraisal interview;
- as part of the developed vetting interview;
- when an employee is under investigation.

**Online questionnaires**

Some organisations ask their employees to complete annual or bi-annual online questionnaires about security issues. These may include questions on personal internet use and presence and ask about 'level of usage', 'internet services used' and 'security awareness'. They may ask subjects to rate themselves on a scale of 1 – 10 in terms of internet knowledge and security awareness.
‘Adverse’ internet usage and presence

When considering how to protect the security and reputation of an organisation from the damage that may be caused by ‘adverse’ internet usage and presence, employers need to consider:

- what types of personal internet usage and/or online material would be considered ‘adverse’ or of concern;
- what the potential impact of ‘adverse’ usage and presence would be on the organisation and its employees;
- how to ensure consistency in the interpretation and reporting of ‘adverse’ internet usage and presence;
- if ‘adverse’ online material is found or if an individual is deemed to be using the internet inappropriately, what are the next steps either in the recruitment process or for the current employee in question;
- how to handle and store the ‘adverse’ online information (in line with the DPA);
- how to minimise the damage caused by ‘adverse’ usage or presence;
- how to reduce the risk of it happening again.

What is ‘adverse’ online usage and presence?

In most cases ‘adverse’ internet usage and presence will be online behaviour that may have the potential to:

- threaten national security;
- damage the reputation of the organisation;
- threaten the security of the organisation and its employees;
- affect the wellbeing of other employees;
- place the individual at increased risk of blackmail, coercion or threat.

Finding ‘adverse’ material online during pre-employment screening

HR, security and vetting professionals may become aware of ‘adverse’ online usage and presence:

- through conducting media checks as part of the pre-employment screening or vetting process;
- by being directly informed by the prospective or current employee during the vetting process;
- by being informed by one or more referees during the vetting process.
Handling and storing online material

Under the Data Protection Act an individual generally has the right to:

- access a copy of the information held in their personal data;
- object to processing which is likely to cause or is causing damage or distress;
- in certain circumstances have inaccurate personal data rectified, blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Act.

According to the Act, employers must ‘handle people’s personal data only in ways they would reasonably expect and make sure they do not do anything unlawful with the data’.15

Employers are advised to apply a consistency of approach when handling and storing online material; the ways in which the material is handled and stored should be the same for all individuals.

If an employer finds information online that is of concern it should be printed, dated and kept as evidence in the event that it may be used in an investigation about the individual in question. For further information about handling and storing personal data, please consult the Data Protection Act and the Employment Practices Code.

‘Adverse’ information cannot be stored indefinitely. Legal advisers recommend destroying what is not needed and retaining anything that might be of further use or required as evidence in investigating an employee of concern.

Assessment

When assessing material found online it is important to be aware that the material is both:

- potentially unreliable, and
- open to interpretation.

According to the Employment Practices Data Protection Code an employer should ‘not place reliance on information from possibly unreliable sources.’16 This includes information found online.

---

15 Data Protection Act
16 Employment Practices Data Protection Code

If an employer has assessed that material found online may pose a risk to the integrity of the role and/or the organisation and that it may therefore affect their employment decision, they must be able to attribute the material to the individual in question. This may involve:

- conducting further media checks;
- talking directly to the individual about their concerns.

**Consistency in interpretation and reporting**

In order to help reduce bias and ensure consistency, comments about the nature of the ‘adverse’ internet usage and/or presence may be written in a reporting document specifically designed for this purpose. In addition, employers may provide media screeners with instructions on how to interpret and report on anything ‘adverse’ they find online.

**Interpretation**

If an employee can directly attribute the online material to the individual in question they need to decide what next steps to take.

Some ‘adverse’ online information can be assessed as potentially more damaging to an organisation and its employees than other ‘adverse’ online information.

If an individual’s online profile suggests that they may be engaging in illegal activities such as viewing and sharing child pornography the employer is legally obliged to inform the police.

If an individual’s online profile suggests that they are engaging in activities that are a potential threat to national security the employer is advised to contact the anti-terrorist hotline on 0800 789 321.

If the online material reveals that an individual has low security awareness and may be vulnerable to social engineering or blackmail, the employer may decide to advise the individual to remove or protect personal information before continuing with the recruitment process.

If the online material suggests that the individual may not be suitable for a specific post for any other reason, the employer is advised to proceed with caution.

**Deciding not to employ someone based on their online usage and presence**

Employment law applies to both those who are job applicants and to current employees. Recruitment decisions should not be based on age, race, gender, sexual orientation, religious or philosophical belief or disability alone. If any ‘adverse’ information found online can also be
interpreted as being specific to any of these attributes an employer may be accused of being discriminatory if they choose to use it as a reason for not employing someone.

According to the Chair of the Law Society’s Employment Law Committee, ‘using (social networking sites) to canvass more information about an employee or an interview candidate is potentially risky for the employer. For example, it is possible to obtain information about a person’s sexual orientation or religious beliefs that can impact or is perceived to impact on the decision made to recruit or not recruit that person – this can lead to discrimination claims.’

It is important to be aware that a candidate can submit a request for access to their file if they wish to find out why they have not been selected for appointment.

Employers need to be confident about their decision not to employ someone based solely on internet usage or presence and to ensure that it cannot be interpreted as being discriminatory.

**Vetting interviews: disclosure about websites of concern**

A recommendation to grant or refuse NSV clearance is made by the government vetting agency to the sponsoring government department who will make the final decision. In some instances the government vetting agency may recommend that vetting status is granted, but reviewed sooner rather than later (e.g. two years instead of three or five).

If an individual and/or one or more of their referees disclose that the individual has viewed and/or interacted with material of concern and further media checks confirm this, then the vetting officer will include this assessment in their report to the sponsoring organisation. If the nature of the material and/or the interaction is of an illegal nature the police will also be informed.

In some cases, it is assessed that what is most important in an individual’s disclosure about internet usage is not necessarily the nature of the internet usage and/or presence, but the fact that the individual is prepared to be open and honest about it.

**Refusal of developed vetting status**

On occasions an individual may be refused developed vetting status based on their internet usage and/or presence or on their lack of integrity in relation to their usage. This is very rarely the sole reason for refusal and is more usually a contributing factor in cases where other evidence suggests a subject’s behaviour and lifestyle are considered inappropriate to the role.

---

17 ‘Using social networking to vet job candidates could land employers in hot water Law Society warns’
Finding evidence of ‘adverse’ internet usage and presence by current employees

Employers may become aware that current employees are interacting with the internet in a way that is deemed ‘adverse’ to the organisation in a number of ways. For example:

- through conducting ‘top-up’ media checks at some stage during employment;
- through direct disclosure by the current employee during appraisal, an informal discussion or during the vetting process;
- from a referee during the developed vetting process;
- from another member of staff who has viewed such material;
- through a reporting hotline.

An employee may be placed under investigation during the course of their employment for a number of reasons. If this occurs an organisation may choose to carry out media checks as part of the investigation and the employee may be questioned about this. This practice must be clearly outlined in an organisation’s policy.

An employee may also be investigated specifically because of their inappropriate internet usage or presence. However, organisations should have clear policy on what they will do if a current employee is assessed to be using the internet in a way that is ‘adverse’ to the security and reputation of the organisation and its employees.

Code of conduct

It is usual practice for an organisation to ask all staff to sign a code of conduct at the commencement of employment. This typically states that if an employee brings the organisation into disrepute they will face disciplinary action. This includes using the internet to do so.

Therefore, if an employer assesses that an employee has bought the organisation into disrepute through their online presence and usage they are entitled to investigate the matter further and if necessary take disciplinary action.

Other online behaviours of concern

An employer may wish to investigate further if there is evidence to suggest that an employee is:

- sharing information via the internet that threatens national security;
- sharing information via the internet that threatens the security of the organisation and its employees;
- sharing commercially sensitive work related information via the internet;
• involved in the online harassment or bullying of another member of staff;
• involved in the online slander or defamation of another member of staff.

This may include:
• sending offensive or threatening emails;
• posting offensive or threatening comments on social networking sites;
• spreading lies and malicious gossip via social networking sites;
• persistently sending emails to someone the individual is attracted to;
• sharing a colleague’s private details online.

Cyber-bullying is a growing problem in the workplace. A survey of 1,072 workers by the Dignity and Work Partnership found that one in five had been bullied at work by email and research has shown that one in 10 UK employees believes cyber-bullying is a problem in their workplace. 18

Source of information

‘Top-up’ checks
If evidence of ‘adverse’ internet usage and presence has been revealed through the practice of ‘top-up’ checks, the employer must have ensured that these checks are proportionate to the role the individual plays and that they have been transparent about their intention to conduct them.

‘Third party’ source
If the information of concern has been received from a ‘third party’ source, either directly or via a reporting hotline service, then the employer must also assess whether the source is credible, the online material genuine and what the source’s motivation is in bringing this information to their attention.

An employer must establish whether the informant is disclosing the information out of spite (do they have a personal dispute with the individual in question or seek to discredit them for other malicious reasons?) and whether they have the organisation’s best interests at heart. In addition, the employer must also ensure that they are neither more or less disposed to believe the accusation due to the race, religion, gender, sexual orientation, disability or age of either the employee being reported on or of the person making the accusation.

The employer cannot rely on reporting from a ‘third party’ source alone and must ensure they have corroborating evidence from an additional source before proceeding with their investigation.

Handling and storing online information

When handling and storing online information that relates to a current employee, the employer should refer to the Data Protection Act and the Employment Practices Code. If the material is of concern to the employer, they should print it, date it and keep it as evidence in case of a future investigation.

Assessment

The online information must be correctly attributed to the employee in question and assessed as ‘adverse’ to the security and/or reputation of the organisation and/or its employees before an employer can ‘act’ upon it.

Consistency in interpretation and reporting

As mentioned above, in order to help reduce bias and ensure consistency, comments about the nature of the ‘adverse’ internet usage and/or presence may be written in a reporting document specifically designed for this purpose. In addition, employers may provide media screeners with instructions on how to interpret and report on anything ‘adverse’ they find online.

Interpretation

If the employee’s internet usage and/or presence is assessed as posing a threat to national security the employer should refer to Section 28 (1) of the Data Protection Act (1998) for information on national security exemptions.19 The employer is entitled to investigate the named individual further and is not required by law to discuss this with them until they feel there is a need to do so.

If there is evidence that the employee has potentially committed a criminal act, the police should be notified immediately. The police will then decide on the nature and extent of its involvement in the case.

If there is evidence that an employee has harassed another colleague via the internet, then the police should be informed. Under the Protection from Harassment Act (1997), the police can act if this has occurred on two or more occasions.20

In other circumstances, if it can be confirmed that an employee is using the internet in a way that is ‘adverse’ to the reputation and/or security of the organisation and its employees, the next step should be to speak directly to the individual in question and, if necessary, advise them to remove any ‘adverse’ online material immediately.

Depending on the nature of the online material and/or the employee’s interaction with the internet, the decision whether to investigate the matter further will now need to be taken.

Investigation

If a disciplinary offence has been committed under the organisation’s disciplinary policy, the investigation should adhere to the requirements set out in the organisation’s disciplinary policy.

Employers wishing to carry out an investigation need to:

- choose the correct people for the task;
- clarify who else is involved, such as HR or line managers;
- consider whether the employee should be suspended during the investigation;
- be mindful of legislation;
- decide how to collect evidence;
- consider whether to monitor the employee, being mindful of internal policies on monitoring of staff.

In order to ensure impartially, it is important that anybody involved, or suspected of involvement, in the unauthorised act is not also involved in the investigation. It is possible, for example, that an employee and his or her line manager are suspected of collusion (in leaking sensitive work information via the internet or in the online harassment or bullying of another work colleague, for example). If this is the case, then the next most senior line manager, or other suitable alternative, should be consulted instead.

It may be that an apparently malicious act has an entirely innocent explanation, so an employee under suspicion should be given the opportunity to explain their actions.

During a formal interview, the employee should be allowed to have one other person of their choosing – a colleague, a union representative or simply a friend from within the organisation – to accompany them. A detailed record of the proceedings should be kept in all cases.

Dismissal

There will be circumstances when it will be proportionate and lawful to dismiss an employee specifically because of their internet usage or presence. An example might be the viewing of child pornography.

If an employee has signed a code of conduct or contract that stipulates they will not bring their employer into disrepute and they have done so online, then it is likely that their employment can be terminated lawfully.
Additionally, if an employee has clearly broken the rules of their contract by harassing or bullying another work colleague via the internet, then the process of dismissal may be more straightforward.

Even if the employee had been found to be accessing material, such as child pornography, outside of work, an employer may still be able to dismiss that employee for bringing the organisation into disrepute.

Legal advice should always be taken when considering disciplinary policies and decisions affecting an employee’s employment.
Encouraging safe and appropriate internet use

In order to help protect the reputation and security of an organisation and its employees, it is important for employers to encourage their staff to use the internet in a responsible and secure way.

This can be done through policy, education and training and could include:

- disseminating messages about safe internet usage via the staff intranet, during the induction of new staff;
- having specific mention of the internet in the code of conduct when agreeing not to bring the organisation into disrepute;
- asking questions about secure internet usage as part of an online security questionnaire and/or annual security test;
- giving defensive briefings about secure internet usage to those staff in roles that are considered high risk (e.g. high profile, high level of responsibility) or who are in locations where there is an increased risk of approach from foreign intelligence agencies or foreign business competitors;
- providing staff with specific advice on how to reduce and control their internet footprint;
- providing staff with specific advice on how to use online social networking sites safely and briefing them on the risks associated with such sites. For example, not posting more personal information than is necessary (including photos), checking privacy settings and thinking carefully about what information they share relating to their job role and where they work.

For more information on the risk of online social networking, see the CPNI guidance: ‘Managing the risk from online social networking’.
Summary

Media screening: an overview

It is becoming increasingly common for organisations and businesses to consider an individual’s online reputation as part of their pre-employment screening, vetting processes and ongoing personnel security procedures.

Although the internet provides a number of benefits when researching background information about an individual, it also increases the security risk to an organisation as personal details shared online can potentially be viewed by anyone else who accesses the internet.

Why conduct media checks?

- to reduce reputational risk to the organisation;
- to reduce security risk to the organisation;
- to confirm identity;
- to reveal information that may be detrimental to the organisation or that would make the individual vulnerable to coercion;
- to ensure that individuals are using the internet securely;
- to help investigate employees of concern;
- to investigate ‘adverse’ internet usage and presence further.

Media screening and the law

There is no specific legal constraint regarding the searching of open source online information. However, there are a number of legal provisions in place to protect privacy and disclosure and against discrimination:

- Human Rights Act (Article 8)
- Data Protection Act (1998)
- Employment Practices Code (helps employers comply with the Data Protection Act)
- Employment Law
- Equality Act (2010)
Fundamental principles of media screening

When conducting media checks the following principles should be applied:

- proportionality
- necessity
- balance and a sense of perspective
- transparency
- consistency of approach
- privacy

Risks associated with media screening

- verification of identity;
- authenticity of material;
- impression management;
- third party views and opinions;
- personal opinion;
- time constraints/amount of material.

When should media checks be conducted?

- media checks are conducted on a role-dependant basis;
- after references have been received and other pre-employment screening checks have been conducted;
- after conducting vetting interviews to check online presence and usage and to further investigate sites of concern;
- ‘top-up’ checks may be conducted during employment as long as employees are clear that this is company policy;
- when investigating an employee of concern;
- when investigating ‘adverse’ internet usage and presence.

Who conducts media screening?

- size and make up of teams conducting media checks varies according to demand and perceived risk;
- media checks may be conducted by HR professionals, security managers and/or vetting officers;
- training on how to conduct open source searches, how to interpret and report on online material may be useful for media screeners;
government vetting agencies conduct media checks and ask questions on internet usage and presence as part of the developed vetting process;
many private sector companies outsource some aspect of their pre-employment screening checks (including media checks) to commercial screening companies.

How to conduct media checks

- search tools that pool people-related information such as 123people.com and Pipl are helpful to use first before checking search engines such as Google;
- search engines such as Google and Yahoo can be useful for further checks, but they may bring up too many hits to check;
- metasearch engines such as Dogpile allow the user to check many other search engines;
- www.news.google.co.uk and www.silobreaker.com are useful for pooling news articles.

‘Adverse’ internet usage and presence

- Employers need to assess what usage and/or presence they consider ‘adverse’, which roles are most at risk from ‘adverse’ internet usage and presence and what to do if evidence of ‘adverse internet usage and/or presence’ is found.
- All personal information relating to an employee must be handled, stored and destroyed according to the Data Protection Act.
- Employers need to ensure that the information they have is authentic and verifiable before proceeding with any further investigation.
- If the information has been provided by a ‘third party’ source, such as another employee, employers must fully investigate their motivation for disclosure before proceeding.
- If an individual’s online profile suggests that they may be engaging in illegal activities, such as viewing and sharing child pornography, the prospective or current employer is legally obliged to inform the police.
- If an individual’s online profile suggests that they are engaging in activities that are a potential threat to national security, the employer is advised to contact the Anti-terrorist hotline on 0800 789 321.
- If an employer decides not to employ someone or to take disciplinary action against an employee or dismiss them based solely on their internet usage and/or presence, they must ensure that this decision cannot be interpreted as being discriminatory.
Glossary of terms

123people
Search tool which searches the internet for people related information (public records, phone numbers, email addresses, images, videos etc). Pipi, zoominfo and wink.com offer a similar service.

Avatar
A computer user’s representation of himself/herself usually taking the form of a three dimensional model. The term comes from the Sanskrit word ‘avatara’ which means ‘incarnation’.

Bebo
An internet based social networking site that is especially popular in Ireland and New Zealand.

Blog
A contraction of the term ‘web log’. A type of website, usually maintained by an individual with regular entries of commentary on a particular subject, descriptions of events or other material such as video clips or graphics. It may also provide links to other web pages and other media related to its topic.

Bunny slipper syndrome
When internet users, in the comfort, privacy and apparent safety of their own homes, volunteer more personal/sensitive/intimate information than they would in other circumstances.

Cracking
Unauthorised use of a computer to tamper with data or programs.

CRB
Criminal Records Bureau

Criminal Records Check (CRC)
Criminal records are maintained by the Criminal Records Bureau (CRB), which has partial access to the Police National Computer (PNC). CRB records are not publicly accessible, and cannot be viewed without the subject's consent (though an employer may make such consent a condition of employment). Information supplied by the CRB depends on the level of disclosure. Low-level disclosures give unspent convictions (i.e. convictions which have not yet been expunged under the Rehabilitation of Offenders Act), while enhanced disclosures ideally include all convictions, cautions, reprimands and final warnings. Enhanced disclosures are typically used to screen applicants for positions which involve contact with vulnerable groups, such as police officers, teachers and social workers.
Cyber-bullying
When the internet, mobile phones or other devices are used to send or post text or images intended to hurt or embarrass another person.

Deep web
The term ‘deep web’ refers to a vast repository of underlying content, such as documents in online databases that general purpose web crawlers cannot reach.

DPA
Data Protection Act (1998)

DV
Developed Vetting: security vetting for those who are likely to have long-term, frequent and uncontrolled access to highly sensitive information or assets. The process includes face-to-face interviews with the individual who requires DV status and with a number of their referees.

Facebook
The most popular western internet-based social networking site. According to Facebook they currently have 500 million users worldwide including 26 million users in Britain – more than a third of the British population.

Flickr
An image and video sharing website.

Hacking
Obtaining and exploiting unofficial access to a computer system.

ICO
The Information Commissioner’s Office.
Responsible for regulating and enforcing the access to and use of personal information.

LinkedIn
A professionally orientated internet based social networking site.

Media screening
Looking at online open source sites in order to research into a subject’s background and lifestyle.

Microblog
A type of blogging, featuring very short posts.

MySpace
An internet based social networking site.

NSV
National Security Vetting
Online reputation
The publicly held social evaluation of a person based on their online behaviour, what they post and what others (such as individuals, groups and web services) share about this person on the internet.

Online social networking sites (OSNs)
Websites such as Facebook that allow users to create their own profile page and interact with other users (known as friends) sharing ideas, activities, events and interests with one another.

Phishing
Fraudsters sending out fake emails pretending to be from a financial institution in an attempt to trick you into divulging logon and account details.

PNC
Police National Computer

Privacy settings
Most OSNs have modifiable settings which allow users to alter how much of their personal information is available to their contacts, other users, third party applications and search engines.

Search engine
Designed to search for information on the World Wide Web. Search results are usually presented in a list of results commonly called ‘hits’. Popular search engines include those provided by Google and Yahoo.

Second Life
An online virtual reality world in which residents can explore, socialise, participate in individual or group activities, create and trade items and services and expand the world as they see fit. Businesses and organisations use Second Life for marketing, entertainment, education and training purposes.

Twitter
A social networking and microblogging service that enables its users to send and read messages known as ‘tweets’. Users can send and receive tweets via the Twitter website or as text messages sent to their mobile phones.

Tweet
Tweets are text-based posts of up to 140 characters displayed on the author’s profile page and delivered to the author’s subscribers who are known as followers.

YouTube
A very popular video sharing website.
Web crawler
A computer programme that browses the World Wide Web in a methodical, automated manner. This process is called web crawling or web spidering. Many sites, in particular search engines, use spidering as a means of providing up-to-date data.
Appendix

Further guidance on internet usage

Internet specific vulnerabilities
The internet facilitates a wide range variety of activities – many are benign in nature. However, some activities may be addictive, anti-social and/or unlawful, such as online fraud, phishing and the distribution of illegal pornographic material.

Addiction to the internet may lead to possible loss of control, stability and change of lifestyle. Excessive internet usage for whatever purpose could have a negative impact on quality of life and may be indicative of other problems that reduce the subject’s capacity to build relationships face-to-face.

Signs of internet addiction may include:

- excessive use of the internet often associated with a loss of sense of time or a neglect of basic drives;
- withdrawal, including feelings of anger, tension and/or depression when the computer is inaccessible;
- the need for better computers, more software, or more hours of use;
- negative repercussions, including arguments, lying, poor achievement, social isolation and fatigue.21

Online pornography

If staff access pornography in the workplace, their employer may find themselves at risk from other employees. In one incident, an employment tribunal found that downloading and viewing pornography in the office by male workers did constitute sexual harassment as it made the working environment unpleasant for a female co-worker, even though it was not directed at her.

The use of a credit card to pay to view pornography is problematic due to the security risk created by sharing personal details, but this also depends on the nature of the material viewed.

Furthermore, some pornography websites may contain viruses, which, if accessed in the workplace, could potentially damage systems.

Game playing and virtual worlds

The internet offers a huge range of games and alternative environments for users to enjoy and to play against other people. In some instances, people join together to form groups or clans.

in order to play on the same teams. Some of these go on to develop their own team websites. Most cases of excessive internet use are associated with online gambling; 12-hour sessions are not unheard of. Such high levels of gaming have also been linked to marital, family and work problems.

Gaming can range from traditional card or board games through to massive multiplayer online role-playing games (MMORPG), which allow millions of people to interact in virtual worlds. The most well known of these is the World of Warcraft series, which has over 12 million subscribers, though games have been also been licensed from films such as The Lord of the Rings, Star Trek and Star Wars.

As well as the MMORPGs, there are also virtual worlds, the most well known being Second Life, which is described as a benign world in which residents can explore, socialise, participate in individual or group activities, create trade items and services and expand the world as they see fit. Businesses and even some countries use Second Life for marketing, entertainment, education and training purposes.

**Internet gambling**

Internet gambling lacks many of the protective mechanisms of real life betting, such as not being able to gamble in a casino when you are intoxicated. Because of speed of feedback, it is also possible that some types of internet gambling (such as roulette) are more reinforcing than real life roulette and there is an increased likelihood of people chasing their losses. Online bookmakers provide the same kinds of bets/service as high street bookies. Spread betting has the potential for particularly high losses and would be a cause of concern.

**Dating sites**

Use of internet dating sites is a popular way of meeting a prospective partner and there are a number of websites that counter for a range of interests and tastes.