17th May, 2012

Social media guidance for civil servants

This guidance was produced as part of the UK Government ICT strategy

Any enquiries regarding part one this part of this document should be sent to emer.coleman@digital.cabinet-office.gov.uk. Any enquiries regarding part two this part of this document should be sent to StevenR.Wilkes@homeoffice.gsi.gov.uk

Government Digital Service | Home Office

INTRODUCTIONS

Francis Maude, Minister for Cabinet Office and Sir Bob Kerslake, Head of the Civil Service

PART ONE

Guidance on the use of social media

For: All civil servants
Covers: How to use social media to communicate and engage effectively
Author: The Government Digital Service, Cabinet Office

PART TWO

Guidance on overcoming the technical barriers to accessing the internet and social media

For: Civil servants who work in ICT
Covers: How to provide the necessary technical infrastructure, platforms and software to enable access to the internet and social media channels
Author: The Home Office

Any enquiries regarding part one this part of this document should be sent to emer.coleman@digital.cabinet-office.gov.uk. Any enquiries regarding part two this part of this document should be sent to StevenR.Wilkes@homeoffice.gsi.gov.uk

Introduction from Francis Maude, Minister for Cabinet Office

The Civil Service is undergoing significant reform and facing new challenges. As part of that process it must embrace new opportunities and technologies that allows it to deliver in different and better ways.

Active engagement with social media encourages different ways of working and opens up the possibility of flatter organisations when communication and knowledge transfer happen in real time. What matters in the world of social media is not so much hierarchy – but hierarchy of contribution. When civil servants, policy makers and service delivery units alike, open themselves to dialogue with the public they can glean a much better understanding of the real needs and concerns of citizens. They can keep up-to-date with the latest thinking as well as being a listening post and avenue for real time reassurance and information.

Social media must be used responsibly and only when it enhances the core work of civil servants. These guidelines give clear and practical guidance on the benefits of social media and how it can be used to enhance policy making and service delivery.

Francis Maude

Introduction from Sir Bob Kerslake, Head of the Civil Service

I am very pleased to see the publication of this Social Media Guidance for Government. As a recent convert to Twitter and Linkedin I can attest to the value of social media channels which I hope have made me more open and accessible to a wide range of people but in particular to our own staff in the Civil Service. I believe in visible leadership and while clearly I can't get to know all of our civil servants, I do want to be known by them and in particular I want them to know that I connect with them and understand the issues that they are experiencing on a daily basis.

There are, of course, legacy, security and infrastructural IT issues that this guidance addresses which mean that not all civil servants can easily access social media channels at this time in their workspaces and we will work over the coming months to address that situation. A job in the Civil Service continues to be highly prized and we can and should aim to be a good employer for our staff. Keeping abreast of new technology and new ways of communicating in a digital era are crucial to our ability to attract a new generation of talented people into the Service. The workplace of the future will have to be less rigid, less hierarchical and a lot more flexible. Participating in social media is a good way to learn how a modern workforce engages and communicates and I hope that more and more of our staff will embrace these new ways of working.

Bob Kerslake

PART ONE

Guidance on the use of social media

For: All civil servants
Covers: How to use social media to communicate and engage effectively
Author: The Government Digital Service, Cabinet Office

Contents

Any enquiries regarding part one this part of this document should be sent to emer.coleman@digital.cabinet-office.gov.uk. Any enquiries regarding part two this part of this document should be sent to StevenR.Wilkes@homeoffice.gsi.gov.uk

1 Introduction

1.1 There are many benefits to using social media. Alongside other communications it can help Government to communicate with citizens in the places they already are; to consult and engage; and be more transparent and accountable. The Government wants to be part of the conversation; understands that it cannot do everything alone or in isolation and will work with those who can and are willing to help.

2 Communicate with citizens in the places they already are

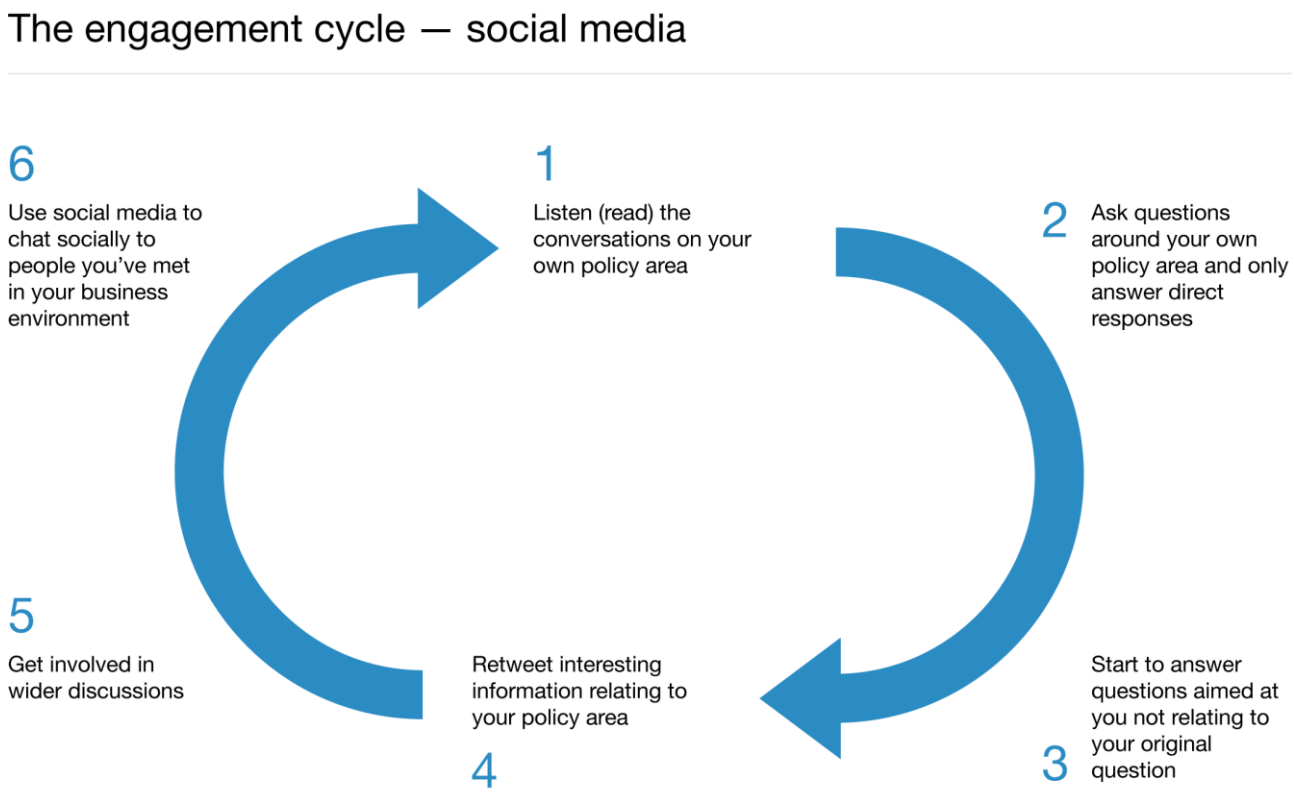
2.1 50% of the UK population are now using Facebook. A recent study showed that people interact with their favourite brands on Facebook more than any other social media network. Increasingly, government is finding that social media has real value when communicating with the public.

2.2 However, the use of social media is not simply a numbers game. The quality of interaction and audience demographics should influence your choice of social media channels. Know who is using different channels and what for and you will know how best to engage with your target audience.

2.3 Sticking to the channels the majority of your audience use will save time, resource and money. But you should also keep abreast of newly emerging channels and use them if you are specifically pointed at them or they contain useful information for key groups.

3 Use social media to consult and engage

3.1 Understanding the engagement cycle on social media (shown below) can help to unravel where online engagement can be useful in the policy cycle. This could include asking questions to crowd-source views, but also something as simple as raising awareness of roundtables and consultation events.



3.2 Use social media to have discussions with your service users or the people whose behaviour you want to change. Ask them to elaborate on the issue, and if you know something that could help, share it with them.

3.3 On the flipside, if you're receiving praise for work done within your team, make sure you pass it on. Social media is one of the few ways you can directly and instantly receive feedback on your policies and decisions.

3.4 Sometimes just listening is as valuable as engaging. Set up quick, easy and free searches to tell you when someone mentions your policy or press release using tools such as Addictomatic or Netvibes.

3.5 Decide whether you want to engage or not based on if one, or both, of you will gain something from the exchange. You don't have to respond to everything.

Increasing the impact of your communications

3.6 You will get far greater traction with your audience if you add a social media layer to your communications - whether in an emergency, for a one-off or more regular events.

> @GAOTG (Get Ahead of the Games) has over 20,000 followers before the Olympics has started - that's 20,000 people awaiting updates from a press team who know something the public need to know. If those 20,000 people feel the update is valuable to them, they will retweet it into the stream of all their followers and the garden fence/word of mouth effect amplifies your message massively. You have a huge potential audience.

3.7 Buzz generated around communications on Twitter can very quickly escalate. Stories and discussions start on Twitter but are quickly picked up, firstly by amateur bloggers, then by professional bloggers, then via news websites and often make it onto the front pages of newspapers 12-24 hours later. You have a real chance to either reinforce or prevent those front-page headlines with the effective use of social media.

4 Use social media to be more transparent and accountable

4.1 Explaining what we do, how we do it and why we do it is already embedded in government through Parliament, public information on government websites and other communications. Social media adds a further level of transparency and accountability to the public.

4.2 It allows citizens to input into decisions, to question them and for replies to be broadcast to many instead of 1-2-1. So government can hear direct from those affected by its decisions – the positive and negative – and explain and/or defend its decisions in response to questions or concerns.

5 Be part of the conversation and all the benefits that brings

5.1 Being present in the conversation means engaging and a core part of any good conversation is listening. There is more value to be gained from engaging in the social media conversation than not - whether you are aiming for cheaper, more personalised service delivery or behaviour change.

The Highway Code Twitter account has over 10,000 followers.

5.2 Communicating 1-to-many rather than repeatedly 1-to-1 directly, quickly and cheaply is one of the major opportunities that social media offers. If you are not aware of rumours circulating within a particular citizen group who use a government service regularly, you cannot address that rumour. But if you are you can get the facts out there quickly and easily.

5.3 Being present in the conversation also allows us to provide a catalyst for the creation of online communities. The community may not exist until a government department or agency creates it. But the community can then evolve with some initial nurturing into a place that is shared with those outside of government who are interested in what you are trying to deliver.

5.4 The community itself can become an authoritative voice providing advice to its members, but in a space that is monitored by government to ensure that the advice given is sensible, relevant and timely.

6 Understand that we cannot do everything alone or in isolation and will work with those who can and are willing to help

6.1 The government wants to play an active part in the social media conversation and all the benefits it brings. But that doesn't mean we need to answer all the queries and questions directed to us via social media.

6.2 Government should not, for example, try to assist everyone who asks a question of us on a Twitter stream. In some cases it won't be appropriate for reasons of impartiality or legality.

6.3 The services and information that government offers exists alongside a network of organisations, such as Not For Profits, Non Government Organisations and others. Many of whom have digital and social media presences that users can be redirected to for information and assistance.

7 Government expects civil servants to adhere to the Civil Service Code online as well as offline

7.1 All civil servants are bound by terms and conditions including the Civil Service Code. The Code sets out the core values - integrity, honesty, objectivity and impartiality – and the standards of behaviour expected of us.

7.2 The principles covering the use of social media by civil servants in both an official and personal capacity are the same as those that apply for any other media. Social media is a public forum and the same considerations apply as would, say, to speaking in public or writing something for publication either officially or outside of work.

7.3 In social media the boundaries between professional and personal can sometimes become more blurred - so it's important to be particularly careful. You are of course free to use social media in your own time but you need to be mindful of your duties not to disclose official information without authority, and not to take part in any political or public activity which compromises, or might be seen to compromise, your impartial service to the Government of the day or any future government.

7.4 Take care about commenting on government policies and practices, particularly those which your own Ministers are responsible for. Avoid commenting altogether on controversial issues affecting the responsibility of your own Ministers, and avoid personal attacks.

7.5 More details are in the Political Activities rules set out in your staff handbook and the Civil Service Management Code. You must comply with any restrictions that have been laid down.

7.6 Remember, once you have posted something on the internet it is very difficult to remove. Check the accuracy and sensitivity of what you are saying before you press 'submit'. Use common sense and if you are unsure about a particular post don't do it and seek advice from your line manager, departmental head of digital engagement or HR team.

7.7 It is important that you are aware that posting any content that is considered inappropriate may result in disciplinary action.

8 Ten tips for using social media

1) Have a clear idea of your objectives in using social media (behaviour change/service delivery/consultation/communication)

2) Learn the rules of each social media space before engaging

3) Abide by the Civil Service Code and ask for advice if you are not sure

4) Remember an official account belongs to the Department not the individual

5) Communicate where your citizens are

6) Build relationships with your stakeholders on and offline – social media is just one of many communication channels

7) Try not to channel shift citizens backwards (move from email to telephone for example)

8) Do not open a channel of communication you cannot maintain

9) Understand when a conversation should be taken offline

10) Do not engage with users who are aggressive/abusive

PART TWO

Guidance on overcoming the technical barriers to accessing the Internet and social media

For: Chief Information Officers, Chief Technical Officers and other ICT professionals in government departments, agencies and arm's length bodies.
Covers: How to provide the necessary technical infrastructure, platforms and software to enable access to the internet and social media channels
Author: The Home Office

Contents

Any enquiries regarding part one this part of this document should be sent to emer.coleman@digital.cabinet-office.gov.uk. Any enquiries regarding part two this part of this document should be sent to StevenR.Wilkes@homeoffice.gsi.gov.uk

1. Introduction

1.1 Social media and the wider internet are becoming increasingly important business tools in helping government departments achieve their objectives. For example, they can be used to facilitate faster and more inclusive two way engagement in developing policy and new services[1]. They can also be used to deliver services; as a means of engaging staff; and as a way of engaging with (or at least listening to) citizens, business and other stakeholders, especially in emergencies.

1.2 The following two quotes from a recent article[2] by Sir Bob Kerslake, Head of the Civil Service, reinforce this:

> **"**Social media is becoming an integral part of the everyday work of the civil servant, opening the Civil Service up and allowing us to be more in touch with our staff and the public than ever before.**"**
>
> "Social media is changing the way government works, and I believe it will have an increasingly important role to play in formulating and delivering government policy."

1.3 Social media is likely to become as ubiquitous as email with many more, if not all, staff eventually needing to use it in some form as part of their work.

1.4 However, greater use of the internet and social media by departments and their staff is often hindered by infrastructure, platform and software issues.

1.5 These guidelines provide a range of potential options which departments could use to overcome some of these challenges so that they are more able to access and therefore exploit the potential of the internet and social media.

1.6 This paper focuses on the challenge of accessing websites external to government, for official purposes. Access to social media and other websites internal to government, or for non-official purposes, is not the focus of the paper. Whilst some of the advice within this document may be useful in those scenarios, many of the issues to consider are rather different.

1.7 These guidelines fulfil Action 30 of the Government ICT Strategy, published in March 2011:

> *To embed social media as a mainstream channel used routinely to engage with citizens, business and internally, the Government will develop practical guidelines on departmental access to the internet and social media channels.*

1.8 In the longer term, some of the major pan-government programmes resulting from the Government ICT Strategy (PSN, G-Cloud, End User Devices, etc.) will need to be designed with greater use of the internet and social media channels in mind. Pending the outcome of that work, these guidelines focus on areas where departments could take shorter term action to start to address their requirements for greater access to these channels. However, they will also provide useful input to the requirements that the major ICT programmes above will need to address.

---

[1] As set out in the Government ICT Strategy:

> *Social media and e-petitions will allow citizens to have increased dialogue and involvement with the Government. This will ensure that policy is developed in consultation with citizens.*
>
> *The Government will use technology to break down barriers and engage with citizens and businesses, bringing innovation to the way in which policy is formulated and delivered. Through greater digitally enabled engagement and collaboration, the Government will create and deliver policy in an open and accessible forum. This will enable citizens to influence, comment on and contribute to the decision-making process.*

[2] http://www.guardian.co.uk/public-leaders-network/blog/2012/may/04/sir-bob-kerslake-social-media

1.9 **This document provides guidance rather than formal policy.** Increased use of the internet, and social media in particular, presents Information Assurance (IA) and cyber risks, such as providing a larger attack surface which could be exploited by an attacker. It is therefore for departments to decide (based on an assessment of the benefits, costs and risks involved, as well as their business needs) which of the suggestions listed they wish to employ. Further guidance on the IA risks can be sought from CESG.

1.10 A combination of the options suggested may be required; departments should consider what is appropriate in their circumstances.

Intended audience

1.11 These guidelines are aimed at CIOs, CTOs and other ICT professionals in the public sector. However, in deciding which (if any) of the options set out in these guidelines to implement, those groups will want to consult with colleagues from their security, HR and business areas, and in some cases also trade unions and CESG. Some decisions may also need ratification at the highest level within the department.

What is out of scope of these guidelines

1.12 These guidelines complement work being carried out by the Government Digital Service in Cabinet Office on how the internet and social media can be better exploited by civil servants and departments. Issues around how the internet and social media should be used to engage with or deliver services to citizens, business and internally are therefore out of scope of this document. For this reason, these guidelines do not make recommendations on who should use social media and how they should do so.

1.13 These guidelines propose ways of tackling the internet and social media access problems currently being experienced by many departments; they are not intended to provide a detailed plan on how to implement them. Such plans will vary considerably across departments due to differences in their existing infrastructures, platforms, software and service provision. However, the guidelines do signpost more comprehensive guidance on individual topics (including useful CESG documents) and provide information on which departments have explored or implemented them.

1.14 In producing these guidelines, a number of issues have arisen around the legal and information management implications of using social media (such as Freedom of Information and liability for what individual employees post). These fall outside the scope of this document, but the need for additional guidance on these issues has been noted.

Disclaimer

1.15 These guidelines have been written as part of the centrally coordinated delivery of the Government ICT Strategy rather than as a Home Office document.

2. The challenges

Legacy web browsers

2.1 Many departments are running legacy versions of web browsers, such as Internet Explorer 6 (IE6). This is commonly attributed to the needs of legacy web applications (for example, HR and finance portals) used in those organisations, which were designed to work with older versions of the browsers.

2.2 Older browsers lack the defence-in-depth mechanisms of the latest mainstream browsers. Modern browsers also implement significant mitigations against many types of attack that either did not exist or were not prevalent when browsers such as IE6 were released a decade ago. In addition, many legacy browsers are no longer supported or less well supported[3].

2.3 Older browsers will also not support modern web technologies, such as HTML5, which are used increasingly to drive social media and other websites. Some older, proprietary browser plug-in technologies, such as ActiveX and Adobe Flash, introduce additional security risks and do not align with the open standards agenda, as set out in the Government ICT Strategy.

No clear and up-to-date understanding of the risks, benefits and costs

2.4 When social media first came to prominence, the risks (in terms, for example, of security, departmental reputation and staff productivity) far outweighed any perceived business benefits. As a result, many departments placed technical restrictions on accessing certain types of websites, including social media sites. However, whilst many of the risks remain, there are now significant benefits to be had by departments from using the internet and social media, as set out in paragraph 1.1 above.

2.5 Similarly, technologies like JavaScript, Adobe Flash and ActiveX were seen to present more of a business or security risk than benefit; so tight restrictions were often placed on their use. Whilst use of these technologies has now started to die out in favour of newer, standards-based alternatives (such as HTML5), many websites still use them and will not function properly without them. Some of these technologies remain inherently insecure, whilst for some the security risks can be mitigated through architectural and other security controls, combined with a pro-active approach to applying security patches.

2.6 Constraints are also often placed on the use of media (video and audio) streaming, primarily due to concerns about security and network bandwidth, both internally and in connecting to the Government Secure Intranet, other pan-government intranets and the internet. But again, the potential business benefits of greater access to media streaming (for purposes such as training and development, participation in web-based seminars and teleconferencing) have increased and there is now a desire for such access.

2.7 However, there remain security risks associated with rendering of media streams, natively, on desktops which are used for accessing information protectively marked as RESTRICTED or higher.

---

[3] CESG has published CESG IA Notice 2010/09 – "Guidance for departments using Internet Explorer" (September 2010), which explains the IA issues relating to the use of older versions of Internet Explorer, it also explains the levels of support available on legacy Microsoft technologies.

2.8 In deciding whether; to what extent; and how access to the internet can be improved, departments need to weigh up the potential risks, the costs of doing so and the benefits to be gained. This, in turn, needs consideration of how the use of the internet and social media can assist in meeting departmental objectives. How social media and the internet are used should, therefore, form part of the organisation's business strategy (or at least its communication strategy) rather than be set out in a separate social media strategy.

Consider alternatives to preventing all usage

2.9 Technical restrictions were put in place by some departments to prevent access to social media sites at least in part due to the potential for time wasting or misuse by staff. However, these restrictions also hinder legitimate business use of the internet and social media channels.

2.10 Whilst some controls are likely to remain necessary, some could be relaxed to facilitate legitimate business use if staff were better educated on the proper use of the internet and social media. Most staff can be trusted to use these technologies appropriately if they are aware of the constraints and risks. And appropriate line management intervention may, in some cases, be a better solution than tighter technical controls that hinder business use.

Existing contractual arrangements

2.11 Departments can also be frustrated in their efforts to make even simple technical changes by sometimes inflexible, risk averse or costly arrangements with system integrators or other ICT suppliers. But some departments, such as HMRC, have already shown that such barriers can be dismantled.

2.12 As well as changes to the actual infrastructure, platform and software, the implications for other elements of ICT service provision (such as the implications for help desks) need to be considered.

3. Possible solutions

3.1 This section outlines a range of possible options for tackling the infrastructure issues that can inhibit access to the internet and particularly social media channels. Some would involve significant projects and expenditure to implement, and would therefore need careful consideration as to whether they are cost-effective, particularly if other planned changes to infrastructures might soon make them redundant. Others are quicker and simpler.

3.2 For a number of the options, there is information on departments that are investigating or have already implemented the option, and information on more detailed guidance to consult, including a variety of CESG and CSOC publications[4].

3.3 Some of these options involve changes to the infrastructure, including the security arrangements. If any of these are to be implemented, it will be necessary to reassess the risks and vulnerabilities, and to consider whether there is any impact on the accreditation of the system and its connection to the GSi.

3.4 Likewise, some of the options would represent significant changes in departmental risk appetite, which might necessitate sign off at senior level.

3.5 The options are:

[4] CESG and CSOC guidance can be accessed on the CESG Information Assurance Portal website https://cesgiap.gsi.gov.uk/index.php. Registration is simple for users on GSi, for those in other situations please contact CESG Enquiries for advice on how to obtain access to the IA Portal.

3.6 Whilst these guidelines do not mandate any of the options, it is recommended that, as a minimum, departments provide staff with access to a modern browser (ideally option A, with option B where necessary in the short term, or option C) and that HR policies are updated and staff educated on how they should and should not use the internet and social media (option I).

3.7 If departments do want to improve access to the internet and social media, then restrictions on what sites can be accessed will also need to be reviewed (option H),

3.8 It is also strongly recommended that all future corporate web applications should, as far as possible, be browser independent and future-proofed (option D).

3.9 Some of the options (such as C, F and H) could be deployed on a role-based or user segmentation approach – i.e. particular capabilities or access to particular sites are only granted to those that have a legitimate business need. This does, however, increase the level of effort required to administer user profiles or permissions, and could lead to dissatisfaction amongst those who are not provided with greater access.

3.10 In line with the Government ICT Strategy, open source solutions should be employed wherever appropriate.

A. Use a more modern[5] version of an internet browser, ideally on a modern operating system

Applicability

A.1 All organisations not using the latest version of an internet browser.

Benefits

A.2 New versions of browsers provide the latest functionality and capability to display websites (including many social media sites) that use the newest web technologies. They can also be better configured to provide optimal access; so, for example, certain functionality can be allowed on trusted sites but not on others.

A.3 CESG strongly advocates running the latest version of a browser, as older versions do not have the security mitigations the newer browsers have. This is because modern browsers are built to defend against attacks "that either did not exist, or were not prevalent years ago."[6]

A.4 For departments running legacy versions of Internet Explorer (e.g. IE6 or IE7), CESG has written a comprehensive guide[7] to migrating to a newer version. It is important that departments still running legacy versions of IE consider this advice, since IE6 is no longer fit for purpose as a corporate web browser and vulnerabilities within IE6 may no longer be patched by Microsoft.

Risks / costs

A.5 Migrating legacy web applications to work in newer browsers may be a difficult challenge, but the IA Implementation Guide from CESG provides practical advice in how to do this for Internet Explorer. The costs of not migrating to a modern browser should factor in the potential increased support costs and the cost of cleanup should a compromise occur.

A.6 In order for the browser to provide the best possible protections, it should be running on a modern operating system. For example, IE8 on Windows XP is not as secure as IE8 on Windows 7. Similarly, IE10 on Windows 8 will have security protections not available in Windows 7.

A.7 To provide maximum security, the browsers themselves, the operating system and any browser plug-ins also need to be regularly updated with the latest security patches.

Further information

A.8 CESG IA Notice – Guidance for departments using Internet Explorer (September 2010)

A.9 Further information on migrating to newer versions of the Windows operating system can be found in CESG IA Notice 2011/11 – Windows XP Migration (June 2011)

---

[5] It is difficult to define "modern" due to the speed at which browsers, and the threats to them, evolve. Departments should be aiming to deploy the latest versions and to regularly update browsers.

[6] CESG Busy reader guide – Upgrading to the latest internet browser (October 2011), p. 2.

[7] IA Implementation Guide No. 5 – Microsoft Internet Explorer Migration (October 2011)

B. Use the "Compatibility View" within newer versions of browsers to enable legacy websites to be viewed whilst upgrading the browsing experience for other sites

Applicability

B.1 For departments that have legacy web applications dependent on older versions of IE, but want to upgrade to a modern browser.

Benefits

B.2 Using "Compatibility View" can enable continued access to legacy applications, whilst delivering the functional and security benefits of a more modern browser.

Risks / costs

B.3 Departments would need to test whether their legacy applications will work using the "Compatibility View" mode.

B.4 The cost and complexity of implementing this solution must be weighed against the cost and complexity of migrating the legacy web applications which are hindering the move to a modern browser. The longer term goal should be to remove reliance of all applications on legacy browsers. Departments should also ensure that new applications are designed to be standards compliant and agnostic of browser technology.

Further information

B.5 CESG's IA Implementation Guide No. 5 – Microsoft Internet Explorer Migration describes a number of ways to migrate off earlier versions of Internet Explorer, these methods have been successfully used by departments including GCHQ.

B.6 Some interest has been shown in plug-ins which allow legacy applications to run in modern browsers. This is not an approach endorsed by CESG.

C. Deploy a second, modern browser and prevent the legacy browser accessing the internet

Applicability

C.1 Departments who are experiencing wider issues in migrating to a more modern browser, especially those still using IE6 and IE7, or those for which options A and B do not provide viable solutions.

Benefits

C.2 The second, modern browser can be used for internet browsing, providing a richer and less vulnerable browsing experience, whilst the older browser still allows access to those corporate systems that rely on it.

C.3 The risks of browsing the internet can be reduced, since the modern browser will provide a greater degree of security.

Risks / costs

C.4 Users may find it confusing to have more than one browser and may try to access internet sites from the old, less secure browser intended only for internal use. Technical safeguards can be put in place to warn users if they try to access the internet from the legacy browser or to prevent them from doing so. Providing specific links to the web pages of corporate applications (for example, on the desktop or in the start menu) may improve usability of this option – essentially making the legacy corporate applications behave like desktop applications rather than allowing general access to the legacy browser.

C.5 A patching process needs to be in place to cover all potentially vulnerable software, including all browsers in use. Supporting two browsers will lead to increased support costs; the long term aim should, therefore, be to migrate to a single modern browser.

C.6 There may be additional demands on help desks.

Further information

C.7 DECC already utilise a second browser (Mozilla Firefox) and the Home Office is planning to deploy Google Chrome.

C.8 DWP currently uses Firefox as a stop-gap measure ahead of moving to a virtualised desktop solution.

C.9 HMRC also uses Firefox as an alternative browser but only to access internal services.

C.10 CESG IA Implementation guide – Microsoft Internet Explorer Migration (October 2011)

C.11 CESG IA Notice – Guidance for departments using Internet Explorer (September 2010)

D. Ensure that, as far as possible, all corporate web applications are browser independent and future-proofed

Applicability

D.1 All departments.

Benefits

D.2 Enables organisations to more easily keep their browser up-to-date, with the benefits outlined under option A above – i.e. greater functionality and better security.

D.3 Reducing the dependence on a single platform and on plug-ins (particularly proprietary ones) reduces the risk of tie-ins to particular suppliers or browsers.

D.4 Use of open standards and technologies improves the ability of departments to share services or applications.

Risks / costs

D.5 Limiting the use of a wide variety of browser plug-ins may impose constraints on services being procured by departments. However, requirements for proprietary technologies are reducing as browsers become more closely aligned with open standards.

Further information

D.6 Departments should cease to build web applications that only work in older browsers or with proprietary plug-ins.

E. Upgrade or review the configuration of corporate web gateways

Applicability

E.1 For all departments, especially those using older web gateway technologies or with a strictly configured gateway policy.

Benefits

E.2 Threats are constantly evolving, as are ways of guarding against them. Modern web gateway technologies may provide increased security whilst providing a better, less intrusive browsing experience. For example, some gateways can selectively remove content rather than block a site in its entirety.

E.3 As well as upgrading web gateways, refining their configurations can have significant benefits – for example, by allowing greater access to trusted sites. Organisations should ensure that any restrictions on internet access are proportionate to potential risk. This could include “black-listing” of sites based on their reputation and content classification, as well as “white-listing” reputable sites. Many modern gateway technologies can update their knowledge of disreputable sites in real-time, providing a quick response to new malicious websites.

Risks / costs

E.4 Upgrading web gateways could be costly and complex, and is likely to be subject to existing contractual agreements.

E.5 Properly configuring new gateways is a far from trivial process and needs careful thought and ongoing management as risks and business needs change.

E.6 To provide maximum security, web gateways need to be regularly updated with the latest security patches.

Further information

E.7 The approach taken to the configuration of web gateways should seek to find an appropriate balance between business requirements and security and policy considerations.

E.8 HMRC have deployed modern web gateway software and found improvements in both security and usability.

E.9 DfT is improving its central firewall to allow control of applications at a more granular level. It is hoped that this will allow access to additional websites, whilst continuing to block threats.

F. Provide employees with mobile devices that provide richer internet access

Applicability

F.1 Departments unable to provide a rich browsing experience from their current mobile devices.[8]

Benefits

F.2 Social media is a dynamic, 24/7 environment and, with more flexible ways of working being introduced, there is often a need for staff to access the internet and social media from mobile devices. In many cases, existing mobile solutions within departments are not adequate for this and staff are already using personal devices such as smart phones, tablets and home computers.

F.3 This does not necessarily mean replacing existing mobile devices. Installing relevant apps onto existing devices and changing security settings may be sufficient to provide the necessary access.

Risks / costs

F.4 The extent to which the information stored on any new devices needs to be managed and backed up, and how can this best be achieved, needs careful consideration.

F.5 Additional cost to the department of providing a second mobile device and inconvenience for staff in having to carry and use two mobile devices. Or, if this is instead of currently provided devices, it introduces an inability for staff to access the corporate network from their mobile device.

F.6 IT and security departments need to manage the risks arising from devices outside the main departmental infrastructure.

F.7 Wi-fi access in departmental buildings would facilitate staff using these devices whilst in the office. Where this cannot be provided through the main corporate network, a separate wi-fi connection to the internet might need to be provided. This would have a side benefit of reducing demand on the corporate network, which could be a significant factor if media streaming is required – see option G.

Further information

F.8 There is growing interest in the use by employees of personal devices to access the internet and social media sites, and potentially even corporate networks. This is generally referred to as “Bring your own device” and is occurring increasingly in the private and local government sectors. CESG are considering this area and expect to publish advice later this month.

F.9 DfT’s Executive Committee has recently given permission for staff in its headquarters building to use their wi-fi network to access the internet from non-secure devices.

F.10 Blackpool Council's supplier reportedly offers both high- and low-security domains for the council's applications. Non-secure devices are allowed access to the latter, giving access to email, secure browser and a staff telephone directory.

---

[8] This option is about replacing or augmenting existing official mobile devices with alternative, officially provided and controlled mobile devices, not about replacing desktop services or providing mobile devices which users can use in an uncontrolled way, as they might use personal mobile devices.

G. Increase bandwidth to enable consumption of richer media

Applicability

G.1 Departments which, either now or in the future, want to allow staff greater access to rich media.

Benefits

G.2 Enables more staff to simultaneously access rich media content (e.g. video streams).

G.3 Increased ability to access video and audio-based training packages; to participate in webinars etc; and to use at-the-desk teleconferencing.

Risks / costs

G.4 Quality of service over internal networks, and on external traffic, needs to be considered to ensure that business critical network activities are not degraded by less critical network traffic.

G.5 If Voice Over IP (VOIP) telephony is also going to be used, this will place even greater demands on the network.

G.6 Departments should assess whether the bandwidth and usage limits that they have in place with their service providers still represent value for money, given the significant reduction of data costs and continual improvements in capacity of service provider networks.

G.7 Internal network infrastructure may need to be upgraded or augmented to cope with increased capacity requirements of increased data usage.

H. Reduce the restrictions on accessing specific internet and social media sites

Applicability

H.1 Potentially all departments that restrict access to the internet and social media sites.

Benefits

H.2 It is extremely unlikely that all such restrictions could be removed, but reducing the restrictions would reduce the technical obstacles to legitimate business use of the internet and social media.

H.3 Helps in developing a culture of trust between staff, their immediate managers and senior management.

H.4 As mentioned in paragraph 3.9, this could be done on a role-based / user segmentation approach. The level of access to certain sites could also be controlled – for example, use of JavaScript can be enabled for specific sites, which allows the experience to be improved for those sites, whilst reducing the risk of scripting attacks on lesser trusted sites.

H.5 In addition, the user experience on some social media sites could also be improved by enabling the storage of session data (e.g. cookies).

Risks / costs

H.6 These channels can be used deliberately or otherwise to upload inappropriate material or malware, or to inappropriately share corporate or personal data. Education and training of staff would be necessary to help combat these threats.

H.7 Employees could waste time. However, a large and increasing percentage of employees possess a smart phone that can be used to access the internet[9] and there are many other ways in which official time or resources could be misused, which managers already manage.

H.8 To mitigate the risks of allowing staff to use a wider range of sites, it may be wise to better monitor internet use so that, where necessary, managers can be provided with the information they need to support any necessary performance management / disciplinary action.

H.9 The security threats, when using richer social media sites, must also be factored into the cost / benefit analysis.

Further information

H.10 CSOC Technology Report: Online Social Networks: risks to UK Government (July 2010)

H.11 CESG Good Practice Guide No. 27 - Online Social Networking (September 2010) – produced in collaboration with the CPNI

I. Update HR policies and educate staff about how they should and should not use the internet and social media

Applicability

I.1 Potentially all departments.

Benefits

I.2 Whilst existing HR and other policies (including the Civil Service Code of Conduct) should apply equally to staff behaviour on-line as well as off-line, many were written before social media became a mainstream tool and how they apply is not always clear[10]. This creates a risk of deliberate or accidental misuse of the internet by staff, and potential difficulties in dealing with such misuse. The updating and publication of policies, and the education of staff, about the use of the internet and social media will mitigate this risk. This should not be just about telling staff what the dos and don'ts are; it is better to empower them to use these services safely and responsibly.

Risks / costs

I.3 Engaging with a wide range of stakeholders (including security, HR, business areas, communication departments and trade unions) in updating and communicating policies is essential.

---

[9] 39% of the UK population now own a smartphone according to the Ipsos Mori *Technology Tracker* (Q4 2011) and this number is rising sharply.

[10] Not all staff recognise, for example, that these sites are not secure, regardless of what privacy or other settings they use.

I.4 The policies and associated guidance need to be simple and relevant, and should not just repeat existing rules. They should also seek to empower staff to behave appropriately rather than discourage them from using social media. Consistency across departments would also be helpful.

I.5 Policies and guidelines must not be just 'shelfware'; they need to be actively publicised so that staff are aware of, understand and adhere to them. And, managers need to actively ensure that they are followed.

I.6 Whilst they should be future-proofed as much as possible (by, for example, making them technology neutral) policies and guidelines will need to be kept under review as technology, and how technology is used, develop.

Further information

I.7 Positive role model behaviour from more senior managers is an effective way of developing the right culture and behaviours.

I.8 The Government Digital Service in Cabinet Office is producing guidance on the use of the internet social media.

I.9 The FCO and HMRC have produced good examples of updated guidelines.

I.10 ACAS has also produced guidelines on producing a social media policy[11].

I.11 The Metropolitan Police has introduced a policy that "*Personal use of the internet is permitted up to the point where it impacts on an individual's ability to deliver their directed tasks.*"

I.12 CSOC Technology Report: Online Social Networks: risks to UK Government (July 2010)

I.13 CESG Good Practice Guide No. 27 - Online Social Networking (September 2010) – produced in collaboration with the CPNI

J. Use audit and monitoring to support alternatives to denying access to social media sites

Applicability

J.1 Any departments that prevent access to social media sites due to concerns about misuse. If a different approach is taken of educating users and trusting them not to misuse the sites (as set out in I), audit and monitoring can be used to verify appropriate use and to support any necessary action where misuse does occur.

Benefits

J.2 If a proactive audit and monitoring approach is in place, then any deliberate or accidental misuse of social media can be identified quickly and action taken to minimise the impact.

J.3 Provides managers with the information on internet usage which can be used for managing performance concerns or in support of disciplinary action.

J.4 Can help to manage greater risks taken in relaxing internet access policies and controls.

[11] http://www.acas.org.uk/index.aspx?articleid=3375

Risks / costs

J.5 There may be privacy, legal and HR considerations in monitoring use of social media for non-business purposes.

J.6 It may be costly to provide an internal capability to police access to social media sites.

J.7 Liaising with key stakeholders (including security, HR and trade unions) in designing new monitoring arrangements and in deciding what outputs are needed and how these could be used will help to prevent issues later.

J.8 The degree of audit and monitoring will depend on the ability to introspect social network connections (e.g. most social network sites are moving towards use of encryption by default).

J.9 Any management information on browsing history etc. that is produced is likely to be subject to Freedom of Information requests.

Further information

J.10 There is a mature market of software that analyses internet usage and provides metrics tailored to business need.

J.11 HMRC's Internal Audit team mine data in an Audit Warehouse looking for potential fraud etc.

J.12 CESG Good Practice Guide: Protective Monitoring for HMG ICT Systems (August 2010)

K. Build architectures which mitigate the risk from rich content websites

Applicability

K.1 Potentially all departments.

Benefits

K.2 Even the most modern browser is not entirely secure but architectures can be developed which mitigate the risks associated with rendering a rich browsing experience. Such architectures avoid the risks of rendering unsafe content natively on a government desktop. The content is rendered elsewhere and presented to the user on their desktop for viewing.

K.3 Users are able to have a very rich browsing experience (using Adobe Flash, JavaScript, etc.) but in a way that does not introduce a risk to their corporate desktop, and therefore to corporate data.

K.4 This technique is commonly used in government systems (including GCHQ and OSCT in the Home Office), it is often referred to as "browse down".

Risks / costs

K.5 There are increased infrastructure costs of providing and managing such a capability.

K.6 Transfer of documents and data between the rich browsing environment and the native desktop introduces IA risks which a department would need to review and manage.

Further information

K.7 CESG Architectural Patterns: Walled Gardens for Remote Access (March 2011)

K.8 CESG Architectural Patterns: Data Import between Security Domains (September 2011)

K.9 DWP's innovation team are considering deploying a sandboxed browser solution.

L. Access corporate social media accounts through a mediation service

Applicability

L.1 Potentially all departments.

Benefits

L.2 Allows for greater monitoring and control of the official use of social media websites (see the benefits for option J).

L.3 This controls access to the login credentials for corporate accounts, whether used by individuals or multiple members of staff. The credentials do not need to be provided to individual members of staff, meaning less overhead when an employee leaves the organisation.

L.4 This service is typically offered as part of a wider social media monitoring package that enables organisations to see what people are saying about them on social media.

Risks / costs

L.5 There is likely to be both a set up and running cost, which could - depending on the number of users - be significant.

L.6 This solution must be sufficiently usable that users do not find an easier alternative.

L.7 The arrangements need to ensure that departmental data does not get locked-in and can be migrated to an alternative supplier or onto departmental systems where necessary.

Further information

L.8 DWP's Communications Directorate has explored the use of social media dashboard monitoring, which has the potential to manage and coordinate communication campaign messaging, and to monitor activity and effectiveness through evaluation metrics.

M. Review the business cases for all standalone computers and networks

Applicability

M.1 All departments that have provided standalone devices or separate networks to access the internet.

Benefits

M.2 Standalone computers and networks are sometimes provided to users who require access to websites not available through the corporate network (e.g. for communication teams in order to maintain a corporate Twitter feed). However, when either alternative ways of accessing the internet are deployed (such as by deploying some of the options listed in this paper) or business needs change, the business case for continuing to use standalones should be reviewed.

M.3 It is greener and probably cheaper to stop purchasing and servicing additional computers and networks.

M.4 Removing standalones can remove the risk of insufficient oversight and compliance with information assurance and management policies (particularly where standalone computers / networks are managed locally by the business unit).

M.5 Standalone computers / networks create usability issues for staff (from transferring material between standalone systems and the corporate networks, to competing with other staff for access to a limited numbers of terminals). Removing the need to transfer data between corporate and standalone systems would reduce the need to use removable media and the associated security risks..

M.6 This suggestion might appear to conflict with option F. However:

i) these guidelines are meant to present a range of ideas to fit the different needs of different organisations; therefore, in some instances they provide alternative ways of dealing with the same problem; and

ii) standalone computers procured and serviced by the organisation are likely to incur significantly more cost than mobile devices.

M.7 IT and security departments need to manage the risks arising from standalone devices and networks, not just those from the main departmental infrastructures. Removal of such standalones will reduce this burden.

Risks / costs

M.8 It is vital that standalone systems are not decommissioned until the business requirement for them no longer exists or can be adequately met by other means such as through the deployment of a second browser or more modern web gateway software.

Glossary of acronyms

ACAS	Advisory, Conciliation and Arbitration Service
BYOD	Bring your own device
CESG	The National Technical Authority for Information Assurance
CIO	Chief Information Officer
CSOC	Cyber Security Operations Centre
CTO	Chief Technology Officer
DECC	Department of Energy and Climate Change
DfT	Department for Transport
DWP	Department for Work and Pensions
FCO	Foreign and Commonwealth Office
GCHQ	Government Communication Headquarters
GDS	Government Digital Service
GSi	Government Secure intranet
HMRC	Her Majesty's Revenue & Customs
HR	Human Resources
HTML	HyperText Markup Language
IA	Information Assurance
ICT	Information and Communication Technology
IE6	Internet Explorer 6
OSCT	Office for Security and Counter-Terrorism
PSN	Public Sector Network
VOIP	Voice Over IP

Any enquiries regarding part one this part of this document should be sent to emer.coleman@digital.cabinet-office.gov.uk. Any enquiries regarding part two this part of this document should be sent to StevenR.Wilkes@homeoffice.gsi.gov.uk

Government Digital Service | Home Office