

## Network Box white paper: Securing social media series

### Part 4: Guide to secure use of Facebook

Huge numbers of companies are banning employees from using Facebook and other social networking sites, concerned about the amount of time wasted on these sites and the drop in productivity as a result. But is this the right way forward? Given the benefits of networking to companies there is a good argument that if correctly used there can be business benefits.

#### **Banning, restricting or allowing Facebook? How to decide**

Before deciding whether to ban Facebook at work, employers should answer the following questions:

- Do you expect your employees to network?
- Do you expect your employees to use business networking sites such as LinkedIn?
- Do you expect your employees to be 'up' on the latest Internet use, such as social networking sites, in the course of their jobs?

If the answer to any of the above questions is 'yes', then banning the use of Facebook, or indeed any other social networking site, may not be the most sensible way forward for your corporate IT policy.

Consider instead:

- Restricting use of Facebook by:
  - Restricted time access to the site, for example during lunch break, and before / after office hours
  - Consider having one or two PCs in a public area, for example a kitchen or café area, where employees can check Facebook. It is much easier to monitor employees who spend all day away from their desk!
  - Restricting tabbed browsing so employees cannot stay logged in to the site all day
  - Monitoring time employees spend on Facebook
  - Making it clear to employees that they are not to use corporate bandwidth by downloading Facebook applications on work networks

Any breach of these rules will result in a ban on that individual accessing Facebook or other social networking sites on their PC or other disciplinary action.

It may be that you can allow certain employees within your organisation different access rights to Facebook – your sales and marketing staff, for example, may use the site to promote product – in which case, consider different access rights for different groups of employees. Each employee should be told exactly what rights they do and don't have.

## Were the answers to the questions, 'No'?

Even if there is no business case for employees using Facebook at work, you may want to consider the following things before introducing an outright ban:

- Staff motivation
  - Would banning Facebook result in a less motivated employee?
  - Would this harm your business results?
  - Would your staff respond better to being given more responsibility for their own results and productivity, rather than 'working to rule' under a ban?
  - Do you want to treat all staff the same, even though some of them don't waste time on Facebook, but access it within acceptable limits at work? Are you grouping all users into the same 'untrustworthy' category?
- Networking opportunities
  - With the imminent launch of 'Facebook business', could you harness the power of Facebook, rather than closing your doors to it?
- Keeping up to date with new marketing or sales opportunities using new platforms to connect with audiences
  - Are you banning your staff from using a platform that would actually allow them to support your business?

## Restricted bandwidth: Add-on applications

Recent reports indicate that in some companies, up to 40 per cent of bandwidth is used through unauthorised applications ([http://news.zdnet.com/2424-9595\\_22-164541.html](http://news.zdnet.com/2424-9595_22-164541.html)). Clearly this is unacceptable. Corporate policy must state that no add-on applications should be used on Facebook; there is absolutely no work-related reason for doing so.

### 1. Wasting company time is against the rules, whatever you're doing.

Employees should be very clear that excessive personal Internet use at work is no more acceptable than spending all day on personal phone calls. Monitor employee productivity and set specific team and individual targets – if they are met, then it doesn't really matter whether an employee is logging on to Facebook. If they are not being met, then this is a clear issue of incompetence on the part of the employee which needs to be addressed, whatever the cause.

## Inform your users

### 1. Education

Consider holding a one-off seminar to explain to employees what is, and what is not acceptable at work. This could include other time-wasting activities, such as long lunches, personal phone calls or personal Internet use, as well as Facebook and other social networking sites.

### 2. Clear Guidelines

- Give clear guidelines as to what is acceptable, such as:
- Personal Internet access is only acceptable outside of office hours, or during lunch breaks
- One or two personal phone calls per day is acceptable; no more Ditto personal emails

This puts Facebook use in the context of other activities that are not acceptable at work. Explain that persistent offenders will be taken through disciplinary procedures.

Add a specific section on social networking sites into your policy on personal email and Internet use, so there is no room for confusion.

### 3. Personal Risks

Educate your employees about the personal risks of social networking sites, including:

- Disclosure of personal details on Facebook, such as date of birth, mother's maiden name, pet's name, key details of home address such as street number and name – all of which can be used to guess personal passwords to online bank accounts, for example.
- Be aware that invitations may not be well intended and answering to everybody is not always the best thing to do.

### 4. Hidden Risks of Association

Make clear that contractual agreements between employee and employer apply to any platform of communication. For example, if your employee has in their contract that they must represent their company in a professional manner, then this applies to any communication on Facebook. So, if the employee lists their company name on their profile, then any action on the site may reflect on the company. You may not, as an employer, dictate how your employee behaves outside the work environment, but you can expect your employees not to allow their behaviour on their own time to be associated with the company's name

## The technology options for businesses

### 1. Restricting access

- Segment employees into who should have what access
- Set access rights via your security system. This would include by username, or active directory group or IP address or IP address range.
- This access it could be set up by department so sales might be allowed more access than accounts.
- Set time access restrictions Set time schedules to govern when the groups defined above are allowed to access social networking sites.

### 2. Denying access to some groups (see above)

### 3. Blocking the ability to download add-on applications

### 4. Consider using quality of service that will limit the bandwidth used for this purpose

This will ensure that Internet access will not be dominated by people using social engineering sites.

### 5. Review the usage made by individuals on the Internet

Your content filtering device should be able to provide a report of the users on your network.

For the latest security information, visit [www.network-box.co.uk](http://www.network-box.co.uk), or read Simon Heron's blog at <http://blog.network-box.co.uk>.