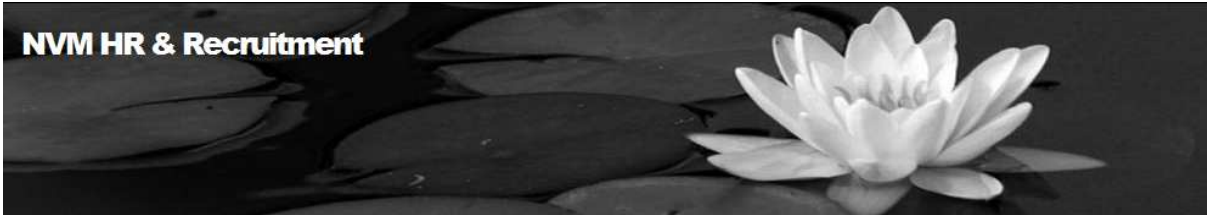


**NVM HR & Recruitment**



# **NVM HR & RECRUITMENT**

## **BRIEFING PAPER**

### **STAFFING ISSUES**

## **Bullying in the workplace - Research and facts!**

Alarming new figures reveal that one in three young women are the victims of workplace bullying. A poll of 685 young women found that 33% had been bullied in the past six months, and the most common culprit was an older woman in a more senior professional position.

More than half believe that bullying has become an acceptable part of workplace culture and more than half said their organisation does not address the bullying problem. In addition, 40% think that bullies are tolerated in the credit crunch environment.

## **Email, internet and IT policies**

A case which came to my attention this month highlighted how using Facebook can get one into a spot of bother with the law. A report of a woman arrested for 'poking' a fellow Facebook user (all well and good when you are genuine friends perhaps), but this particular lady had a restraining order against her and 'poking' her victim was deemed to be in breach of this!

Clearly this is an extreme example of an individual who was seemingly pretty careless when it came to understanding the power of social networking, but what about policing usage in the workplace? As social networking becomes more and more prevalent both inside and outside the workplace I thought I would look at the areas you may want to cover in Email, Internet and IT policies to protect your organisation.

## **Personal Use of Internet and Email**

You may want to prohibit personal use completely or simply set out fair usage policies which you then trust staff to respect. Generally it would be sensible to prohibit the use of the internet for non work related matters during working hours.

It is also sensible to set out your expectations in terms of appropriate sites/material to be accessed at work, e.g. no offensive material to be viewed, downloaded or circulated. Some guidelines as to what may be considered offensive could also be useful (although you may not want to be too explicit!)

Some organisations have filters on email and this can be a good precaution if you are particularly concerned about the nature of email that may be leaving (and entering) your servers.

## **Social Networking**

It would be worth deciding whether you want to embrace cyberspace as another way of reaching potential contacts or not and advising your staff accordingly. There are various business networking tools which fall under the social networking umbrella, such as LinkedIn and even Twitter. As with all other forms of communication that link individuals to your Company you may wish to have some control over the type of material and wording that is posted on these sites; if so it would be worth setting this out in a memo or your IT policy so that expectations are clear.

Equally you may want to consider who the contacts that are developed on networking sites belong to should an employee leave the business. You may be able to make a firmer claim on contact lists if you expressly state that they will be deemed as being Company intellectual property as they were developed during employment.

You may also want to spell out that you will expect staff to remove anything from their profiles that associates them with your Company if their employment ends so that they are not falsely purporting to still work for you (which may even be in breach of their contract).

Finally on this point, it was reported a few weeks ago that some IT experts believe that it is just a matter of time before organisations will start enforcing uniform or dress code policies on employees' online avatars (i.e. their computer generated representations of themselves). This might sound a bit extreme, but if you believe that staff may be using symbols/avatars to represent themselves online that are not compatible with your corporate or professional image and their profiles can be linked back to the Company then you may want to consider providing some guidelines.

## **Enforcement**

Rather than leaving it all to the IT bods to tell you that something funny has flashed up (although hopefully not literally!) I would recommend that you ensure that all managers and staff are aware of the guidelines and the need for enforcement. I am not suggesting that you encourage a culture of snitches, but the idea that making sure that inappropriate usage or images do not occur is everyone's responsibility is a good idea.

In your policy it is important to be very clear about what is and is not acceptable and what the consequences of a breach of the policy may be. By having some examples, although indicating that it is not an exhaustive list you would be clearly demonstrating that you have given fair warning. Needless to say in applying the rules consistency would as ever be key!

**If you have any queries about this update or feel that you would like help with either drawing policies up or with a particular employee issue related to IT usage or any other HR related matter please do not hesitate to get in touch:**

**Call me on 01243 533 150 or visit [www.nvmrecruit.co.uk](http://www.nvmrecruit.co.uk)**

Natalie Thompson

---

### **COPYRIGHT:**

This publication is the copyright of Independent Examiners Ltd. and may not be reproduced without permission. If you would like to reproduce or publish this material, permission should be sought in advance by emailing [support@iel.org.uk](mailto:support@iel.org.uk) or telephoning 01243 555611

### **DISCLAIMER:**

This guide is intended only to give very general advice in relation to the topics covered. These guidelines should not be relied upon as a substitute for obtaining specific and more detailed advice in relation to a particular matter.