

**This is a sample – not the full document**

**Buy the full document in Word format.  
Select from the following options:**

**Individual Document**

<http://www.compactlaw.co.uk/internet-and-email-policy.html>

**Employers Pack**

<http://www.compactlaw.co.uk/employers-pack.html>

**Workplace Pack**

<http://www.compactlaw.co.uk/workplace-pack.html>

## **INTERNET AND EMAIL POLICY**

These guidelines for Internet and email usage form part of your terms and conditions of employment at *[Insert Organisation name and address]*, ("the Organisation").

These guidelines apply to your employment at the Organisation and all other Organisation sites that you may be asked to work at from time to time. These guidelines must also be observed when visiting and using client or partner facilities. Employees must also comply fully with whatever guidelines exist at client or partner sites.

Please note that these guidelines also apply to you if you are working as a contractor, agency worker, temporary worker or volunteer within the Organisation.

For any guidelines to be effective they must be applied throughout the Organisation and apply to all staff regardless of position or seniority.

If you have any questions regarding these guidelines and how they apply to you please consult *[Insert manager's name]*, *[Insert manager's position]* before taking any action that may breach these guidelines.

### **1. Minor Breaches**

Minor breaches of these guidelines shall constitute a disciplinary offence and will be dealt with using the disciplinary procedures of the Organisation.

### **2. Serious Breaches**

Serious breaches of these guidelines shall constitute gross misconduct and shall allow the Organisation to terminate your employment, immediately, without notice. Or terminate your contract immediately without notice if you are a contractor, rather than an employee.

### **3. Monitoring**

**3.1** The Organisation reserves the right to monitor all external and internal communications and access to the Organisation network, intranet and the Internet, (as applicable) where the property of the Organisation is used in the communication or is accessed remotely from outside the Organisation. This includes the use of portable computers and mobile devices, including mobile phones issued to the employee by the Organisation.

**3.2** The Organisation reserves the right to use the following methods for monitoring of communications:

Fileserver log file analysis.

Data packet analysis.

Email message analysis, including content of individual emails and attachments where required.

**3.3** The Organisation shall assess the impact of any monitoring or extension to existing monitoring within the Organisation prior to its introduction. Any assessment will consider the following:

**3.3.1** The reason for implementing or extending monitoring and whether it is justified;

**3.3.2** The likely adverse impact on employees and third parties communicating with the Organisation;

**3.3.3** The use of alternatives to monitoring or alternative methods of monitoring;

**3.3.4** Any additional obligations that arise due to the monitoring, for example the secure storage of and access to information gathered by monitoring;

**3.4** The Organisation will also consider the impact of monitoring on employees such as:

**3.4.1** The risk of intrusion into employees' private lives;

**3.4.2** The extent to which employees will be aware of the monitoring;

**3.4.3** The impact monitoring will have on the relationship between employees and the Organisation;

**3.4.4** How monitoring will be perceived by employees.

**3.5** The Organisation shall inform all workers prior to the introduction of any such monitoring or the extension of any existing monitoring. Furthermore the Organisation will inform individual workers if their communications are being specifically monitored or accessed. However, an individual will not be informed where serious breaches of the policy or criminal activity is suspected and where informing the individual would hamper any investigation or risk the loss of data and evidence.

**3.6** The Organisation shall take all reasonable steps to ensure that personal communications are not accessed during monitoring. However, the Organisation can

access personal communications where such communication are partly used to pass information belonging to the Organisation or where the nature of the personal communication provides evidence of the breach of this communications policy.

**3.7** The Organisation shall not be liable for any breach of privacy should any communications of a personal nature be found and accessed by employees of the Organisation or third parties authorised by the Organisation and acting in the course of their employment.

**Sample document – the remaining are clause headings only**  
**Full document contains all clauses**

**4. Usernames and Passwords**

**5. Internet Usage**

**6. Social Networking Sites**

**7. Personal Blogs & Micro Blogging**

**8. Password Protected Areas**

**9. Email Usage Guidelines**

**10. Emails are Permanent**

**11. Proper Deletion of Emails from your PC**

**12. Email Signature File**

**13. Email Etiquette**

**14. Third Party Products and Software**

**15. Downloads and Attachments**

**16. Transportation and Security**

**17. Organisation Access**

**18. Date of Implementation**

**19. Questions**

**20. Alteration of these Guidelines**

(c) <http://www.compactlaw.co.uk>

<http://www.compactlaw.co.uk/internet-and-email-policy.html>