Computer & Internet Policy

Computer use
Many employees have access to computers in and outside the workplace for the use by them and the children in connection with the company's business. The company expects certain standards of professional conduct to be observed by employees, students and other designated persons in order to protect the company's legitimate business interests and to ensure children are safeguarded at all times from the dangers of inappropriate use.

Acceptable e-mail and internet use
Use of the email and internet by employees is permitted and encouraged where such use supports the goals and objectives of the business.

However, the company has a policy for the use of the email and internet whereby employees must ensure that they:

- comply with current legislation
- use the internet in an acceptable way for business purposes
- do not create unnecessary business risk to the company by their misuse of the internet

Children's use
Today's children are more knowledgeable than previous generations in understanding the workings of computers and in finding their way around the internet. Whilst we would never seek to prevent children from developing their IT skills we must be wary of the hidden dangers that face children in using the internet and children's naivety in these matters. Therefore we have taken the following precautions to safeguard them:

- use of a content control solution across all settings
- use of passwords by staff so they know when children are accessing computers
- regular but not intrusive monitoring by staff during children's usage

Unacceptable behaviour
In particular the following is deemed unacceptable use or behaviour by employees and students:

- use of company communications systems to set up personal businesses or send chain letters
- forwarding of company confidential messages to external locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the corporate network

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to access any live TV broadcast which would contravene the TV licensing laws
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about the company, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format (see also Social Networking)
- revealing confidential information about the company in a personal online posting, upload or transmission - including financial information and information relating to our customers, children, business plans, policies, staff and/or internal discussions
- introducing any form of malicious software into the corporate network
- using the e-mail to inadvertently form a contract on the company's behalf

Social Networking – professional conduct

The company recognises that employees may keep personal web pages and interact using social networking sites (Facebook, My Space, You Tube, Bebo, Twitter etc). We therefore need to ensure employees are aware of our expectations in their professional conduct:

- social networking sites must not be accessed via company computers or mobile phones. When accessing via personal mobile phones this must only occur during breaks and not within working hours
- employees must not post information which is confidential to the setting, individual children, other staff or parents
- employees must refrain from making references to the setting, children, other staff and parents which are derogatory, defamatory, discriminatory, inappropriate, unsubstantiated or offensive in any way to anyone and which may bring the company into disrepute or affect its reputation
- any entries made by an individual will have been deemed to have been made by them personally, unless they can definitively prove otherwise and may be used by the courts for litigation purposes
- if staff have any parents accessing their pages on social networking sites then this relationship must remain professional at all times and must not contain any reference to the company, other staff or children

Monitoring

The company accepts that the use of email and the internet are a valuable business tools. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's email and internet-related resources are provided for business purposes. Therefore, the company maintains the right to examine any systems and inspect any data recorded in those systems and to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and

- To promote productivity and efficiency.
- To ensure there is no unauthorised use of the Company's time.
- To ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment under the terms of the Company's grievance policy

Company-owned information held on third-party websites
If you produce, collect and/or process business-related information in the course of your work, the information remains the property of the company. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Computer software
The Company licences the use of computer software from a variety of outside companies. The Company does not own this software or its related documentation and, unless authorised by the software developer, neither the Company nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Any employee found to be contravening this may face disciplinary action under the Company's disciplinary procedure.

Computer games
There are computer games on the network. Employees may only access these outside their normal working hours, for example during lunch breaks, this is not deemed "personal".

Computer viruses
The Company's computer network makes it vulnerable to viruses. Therefore, only duly authorised personnel have the authority to load program software onto the network system. Data compatible with the Company's system may be loaded only after being checked for viruses by authorised personnel. Any employee found to be contravening this may face disciplinary action under the Company's disciplinary procedure.

Computer Health Checks
A Computer Health Check Procedure is available and should be followed accordingly.

Disciplinary Action
Employees whose conduct breaches this policy in any way will be subject to disciplinary action in accordance with the company's disciplinary procedure up to, and including, dismissal.

Any blog entries made inside or outside the workplace that are defamatory, derogatory, or discriminatory about the setting, its parents, children or employees will be investigated as gross misconduct. If substantiated, such conduct may lead to summary dismissal after the due process of the setting's disciplinary procedure has been followed.

Vandalism of the Company's computer network constitutes a potential gross misconduct offence and could also render the employee liable to summary dismissal under the Company's disciplinary procedure.

Agreement
All company employees, contractors or temporary staff who have been granted the right to use the company's internet access are required to sign an agreement confirming their understanding and acceptance of this policy.