BARNFIELDS EXTRA

Barney Bears Nursery

Acceptable use of computer facilities, email and the internet

The Company has published guidance on the acceptable use by staff of Barnfields Extra's computing facilities. The guidance is intended to support the use of computers by staff in their work, and to protect both individual members of staff and their work, and the Company, its systems and its resources. This document summarises the guidance.

General

- You may make reasonable personal use of computing facilities provided by the Company. This personal use should not interfere with the performance of your duties or cause any damage or difficulty to computers or to networks, or any difficulty or distress to others.
- You must use computing facilities in a reasonable manner. You must not install inappropriate software and you must not reconfigure any machine you have access to against the advice of the appropriate authorised member of staff. If in doubt you should seek the advice of the appropriate authorised member of staff.
- You may not make substantial use of the Company's IT facilities for private financial gain or for commercial purposes outside the scope of official duties or functions without specific authorisation to do so.

Internet usage (including e-mail, the Web, chat rooms)

- You may make reasonable use of the Web for other than strictly work purposes provided it does not adversely affect your work and the work of others and has a minimal effect on the Company's resources.
- You may make reasonable use of Company facilities for personal e-mails, provided that this does not have more than a minimal impact on resources and does not adversely affect your work or the work of others.
- If an e-mail message is personal, you may wish to make this clear by using the word 'personal' in the subject line.
- When you send e-mail, you should remember the following:
    i. An e-mail message is legally equivalent to a letter. E-mail messages can be defamatory and can form contracts. For these reasons it is important to take the same care composing e-mail messages as letters.
    ii. E-mail messages, like other documents, can be disclosed to the person they are about under the Data Protection Act and in the event of legal proceedings.
    iii. Messages may be seen by system managers and other IT support staff, just as postcards may be seen by postal workers. Moreover, the Company cannot guarantee that communications will not be accessed illicitly.

Security and protection of information

The main points to be aware of in the context of computer use are:

- You should guard confidential material and personal information by the proper use of passwords and other security measures.
- Not all computer systems are suitable for the storage of confidential information. You can get advice on this from the appropriate authorised member of staff.
- You can protect highly sensitive material through the use of encryption.
- You must not disclose passwords or other access codes to other persons.
- You must comply with the Data Protection Act, which requires that the Company keeps personal information secure.
- When working with confidential information, you must take care not to leave it inappropriately on screen. You should not leave your computer logged on when unattended, unless it is in a secure location.
- You should observe the same standards of confidentiality for electronically held or generated information as for information held on paper.

If you have a concern about the inadequate protection of data, you should inform line manager so that any necessary steps can be taken to safeguard the data.

All members of staff have an obligation to protect data and systems by following up-to-date recommendations to avoid damage from viruses and other malicious programs. .

Misuse of computing facilities

As stated above, the Company permits reasonable personal as well as professional use of computing facilities. You should be careful not to misuse these facilities, for instance by:

- Hacking — attempting to access systems or information within or outside the Company without authority, or encouraging others to do so.
- Deliberately accessing from the Internet material which is counter either to legislation, Company rules or policies (e.g. equal opportunities) or to commonly accepted standards, or is likely to be offensive to reasonable people. Members of staff may access this kind of material only for bona fide academic purposes. However, accidental access to such sites can take place; if you are concerned that such accidental access has taken place you may wish to report your concerns to an appropriate person.
- E-mail communications which constitute bullying or harassment, as defined in the Company's Code of Conduct Policy.

Investigation of misuse and interception

The Company needs procedures in order to be able to investigate any suspected misuse of computing facilities. Investigators may need to inspect any files held on any of the Company's computing systems. These procedures will be applied infrequently and in a strictly controlled manner. Where inspection is deemed to be necessary, the Chairman shall give permission for such access. If there is a need to access files, the individual member of staff will normally be asked for his/her consent. However, in certain circumstances, exceptionally it may be necessary to obtain access without consent,

i. if urgent access is critically required for operational purposes but the member of staff is absent and cannot be contacted,
ii. if there is prima facie evidence that a member of staff may be misusing facilities to an extent which would be considered serious or gross misconduct or if there is a need to initiate an investigation and there is a serious possibility that evidence might be destroyed.

The procedures set out above will be used only where there is an urgent operational need and the member of staff cannot be contacted or where there is prima facie reason to believe that misuse may have occurred. The privacy of individuals will be respected in other situations, and that privacy will be protected especially in connection with the areas defined in the Introduction. In the case of e-mail, normally subject headings only will be scanned, and the content of the messages will be read only where (in connection with item (i)) it is established that the message is one sent or received as part of the individual's duties as a member of staff or (ii) a prima facie case of misuse has already been established. While strict application of this principle cannot be guaranteed for arbitrary files (i.e., computer files other than e-mail) it will be used as a guide.

As part of normal procedures, computers linked to networks may be scanned automatically for vulnerability and the Chairman may authorise the routine monitoring of Internet access generally, including e-mail traffic volume (but not content).

Misuse and disciplinary action

The Chairman will decide in the light of the outcome of an investigation of possible misuse of computing facilities whether disciplinary action is appropriate, and if it is judged appropriate, instigate necessary action in accordance with the relevant disciplinary procedures concerned.