Acceptable Internet Use Policy

Legislation

• Data Protection Act 2018

Related policies

• Whistleblowing

• Social networking

• Safeguarding children and child protection

• Online safety.

This policy describes the rights and responsibilities of staff using resources such as computers, tablets, the internet and mobile telephones. It explains the procedures you are expected to follow and makes clear what is considered acceptable behaviour when using them. These devices are a vital part of our business and should be used in accordance with our policies in order to protect children, staff and families.

Security and passwords

All electronic devices will be password protected and passwords will be updated on a regular basis. Passwords for our systems are confidential and must be kept as such. You must not share any passwords with any other person; in particular you must not allow any other staff member to know or use your password.

Email

We expect all staff to use their common sense and good business practice when using email. As email is not a totally secure system of communication and can be intercepted by third parties, external email should not normally be used in relation to confidential transactions. Emails must not be used to send abusive, offensive, sexist, racist, disability-biased, sexual orientation based or defamatory material, including jokes, pictures or comments which are potentially offensive. Such use may constitute harassment and/or discrimination and may lead to disciplinary action up to and including summary dismissal. If you receive unwanted messages of this nature, you should bring this to the attention of the manager.

Internet access

You must not use the internet facilities to visit, bookmark, download material from or upload material to inappropriate, obscene, pornographic or otherwise offensive websites. Such use constitutes misconduct and will lead to disciplinary action up to and including summary dismissal in serious cases. Each employee has a responsibility to report any misuse of the internet or email. By not reporting such knowledge, the employee will be considered to be collaborating in the misuse. Each employee can be assured of confidentiality when reporting misuse.

Personal use of the internet, email and telephones

Any use of our electronic communication systems (including email, internet and telephones) for purposes other than the duties of your employment is not permitted.

Emergency personal calls need to be authorised by the manager and, where possible, be made on your own personal mobile phone outside the nursery. Disciplinary action will be taken where:

• The privilege of using our equipment is abused, or

• Unauthorised time is spent on personal communications during working hours.

Data protection

When using any of our systems employees must adhere to the requirements of the General Data Protection Regulation 2018 (GDPR). For more information see our Data protection and confidentiality policy.

Downloading or installing software

Employees may not install any software that has not been cleared for use by the manager onto our computers or systems. Such action may lead to disciplinary action up to and including summary dismissal in serious cases.

Using removable devices

Before using any removable storage media which has been used on hardware not owned by us (e.g. USB pen drive, CDROM etc.) the contents of the storage device must be virus checked.

This policy was adopted on	Signed on behalf of the nursery	Date for review
23/01/2026	Heather Black	23/01/2027