Acceptable IT use policy

At Raised In it's our duty to ensure that all team members are qualified and/or have relevant work experience and enthusiasm for working in early years. All team members are required to provide a recent or complete a new Disclosure and Barring Service (DBS) check. They must also provide Raised In with two relevant and recent references, one of which must be their current/previous employer or college tutor. Original copies of all qualification certificates are required, and a photocopy of each is kept on file.

This Policy describes the rights and responsibilities of Raised In team members when using resources, such as computers, tablets, the internet, landline and mobile telephones, and other electronic equipment. 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, team members and families.

Security and passwords

All electronic devices will be password protected and passwords where appropriate 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 team member to know or use your own personal password. Where relevant, two-factor authentication will also be used.

Email

We expect all Raised In team members 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.

Email should never 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 your line manager.

Where appropriate when sending confidential information to third parties such as Local Authority this should be sent through secure email or password protected method.

All work-related email communications will be sent through a Raised In email address and no personal email will be used.

Internet access

Team members 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 team member will be considered to be collaborating in the misuse. Each team member 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 Raised In equipment; 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 (GDPR) and Data Protection Act 2018. For more information see our Data Protection and Confidentiality Policy.

Downloading or installing software

Employees may not install any files or 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 Raised In (e.g. USB pen drive, CDROM etc.) the contents of the storage device must be virus-checked.

Removable devices must not be taken home unless under exceptional circumstances and authorised to do so by the management team, with prior written permission and risk assessment in place.

Signed: Nicola Brimble, Head of Nursery

Date: 01 December 2023

Review Date: December 2024

This policy links to: Electronic and Online Safety Policy, Safeguarding policy and Data Protection and Confidentiality Policy