Acceptable Internet Use Policy

Legislation

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679).

Related policies

- Whistleblowing
- Social networking
- Safeguarding children and child protection
- Online safety
- Information security

This policy describes the rights and responsibilities of staff using resources such as computers, tablets, the internet, landline and mobile telephones, approved Artificial Intelligence (AI) tools, 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, staff and families.

This policy should be read in conjunction with the Cyber security policy.

Security and passwords

All electronic devices will be password protected and passwords will be updated every six months for systems that contain personal data or on a regular basis for all other systems. Passwords must not be reused. 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. Passwords will be stored using password managers with end-to-end encryption. Accounts will be removed immediately when a staff member has left employment.

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 your manager. Staff will receive training in recognising when emails may contain spam, phishing or other harmful content. Staff must report suspicious messages or links to management or IT support. Accounts will be removed immediately when as staff member has left employment.

More information can be found in the information security policy which will be provided upon request.

Emails containing information about children should include only the minimum necessary details. When referring to a child, use initials and date of birth instead of full names. If more information needs to be shared, place it in a locked attachment and send the password in a separate follow-up email.

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 must not install any software that has not been cleared for use by the manager or IT support 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. No unknown USBs or external devices will be used.

Use of Artificial Intelligence (AI) tools

AI tools may support staff with drafting, summarising, organising information, and generating wording suggestions. They must always be used safely, responsibly, and in line with safeguarding and data-protection obligations.

Approved AI Tools

- Microsoft Copilot (company devices + logins only)
- Famly Sidekick (within Famly platform)

No other AI platforms, apps, personal accounts or external AI tools may be used

Principles of AI Use

AI may be used to:

- Support and improve staff workload
- Assist with planning and drafting
- Summarise or rephrase information
- Provide inspiration for wording

AI must not be used to:

- Replace professional judgement
- Produce unchecked final documents
- Create externally shared content without human review
- Make decisions affecting children, families, or staff

Data Protection when using AI

You must limit the data that is entered into any AI system to that which is strictly necessary. Where personal or identifying data needs to be entered it should be limited and wherever possible anonymised.

Safeguarding Restrictions

AI must never be used to:

- Draft safeguarding or incident reports
- Analyse behaviour or developmental needs

- Draft identifiable child observations
- Create images of children, families, or staff
- Generate images of real people
- Make assessments or decisions impacting a child