Acceptable Internet Use Policy

Nurture and Grow Childcare

Purpose

This policy sets out the responsibilities of staff in using electronic devices and communication systems, including the internet, email, mobile phones, and social media. It aims to protect children, staff, and families by ensuring safe, lawful, and professional use of technology. 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.

Legal Framework

This policy complies with the following:

- Statutory Framework for the EYFS
- Children Act 1989 and 2004
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Equality Act 2010
- Prevent Duty Guidance
- Working Together to Safeguard Children

Related policies

- Safeguarding and Child Protection
- Data Protection and Confidentiality
- Whistleblowing
- Online Safety
- Social Networking
- Staff Code of Conduct

Acceptable Use Responsibilities

Security and Passwords

- All nursery devices are password protected.
- Passwords are confidential, updated regularly, and must not be shared.
- Access to confidential data is strictly limited to authorised users.

Acceptable Internet Use Policy

Nurture and Grow Childcare

Email Use

- We expect all staff to use their common sense and good business practice when using email. It must be used professionally and only for work-related communication.
- Sending or forwarding discriminatory, defamatory, or offensive content is strictly prohibited and will result in disciplinary action.
- Staff must report inappropriate emails to management immediately.

Internet Use

- The internet must not be used to access inappropriate, pornographic, violent, or extremist content.
- Misuse will lead to disciplinary procedures, including possible dismissal.
- Each employee can be assured of confidentiality when reporting misuse.

Use of Social Media and Mobile Phones

- Personal mobile phones must not be used during working hours in areas where children are present.
- Staff must never post images or confidential information about children or the nursery on personal social media accounts.
- The nursery's social media accounts are managed by authorised personnel only.

Personal Use

- Personal use of nursery equipment (phones, computers, email, internet) is not permitted during working hours.
- Emergency personal calls must be approved by the manager and made outside of working areas.

Data Protection and Confidentiality

- All staff must comply with UK GDPR and the nursery's data protection policy.
- No personal data may be stored on personal devices or removable storage unless authorised and encrypted.
- Email should not be used to send unencrypted confidential or personal information.

Acceptable Internet Use Policy

Nurture and Grow Childcare

Software and Removable Devices

- Only authorised software may be installed on nursery systems.
- All external devices (USB drives, external hard drives) must be virus-checked before use.

Monitoring and Reporting

- Use of digital systems is monitored to safeguard children and uphold policy.
- Staff must report breaches, misuse, or suspected online abuse to the DSL or management.
- Failure to report known breaches will be treated as misconduct.

Disciplinary Action

Examples of misuse include:

- Accessing or distributing offensive material
- Using nursery devices for unauthorised personal use
- Breaching data protection obligations
- Inappropriate social media conduct
- Violations may result in disciplinary action, including dismissal.

Policy Review

This policy will be reviewed annually or when there are significant legislative or regulatory changes.

This policy was adopted on	Signed on behalf of the nursery	Date for review
27th July 2025	Tracey Doidge	*27th July 2026*