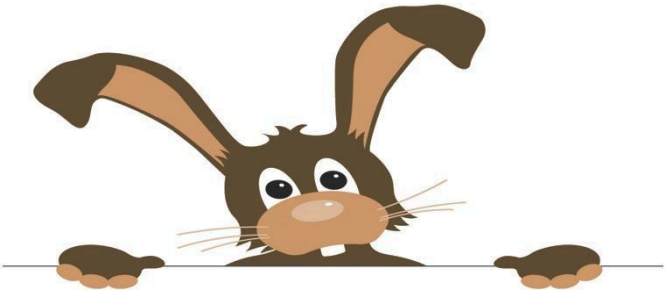

Acceptable Internet Use policy

The internet should be considered part of everyday life with children and young people seeming to be at the forefront of this on-line generation. Knowledge and experience of information and communication technology (ICT) should be considered an essential life skill. Developmentally appropriate access to computers/IPADS tablets and the internet in the early years will significantly and positively contribute to children and young people's enjoyment of learning and development.

Children and young people will learn most effectively where they are allowed managed access to computers/other devices and control of their own learning experiences, however such use carries an element of risk. Early Years Manager, deputies and Educators, in partnership with parents and carers, should consider it their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep children and young people safe, without limiting their learning opportunities and experiences.

Policy statement

This policy will outline safe and effective practice in the use of the internet. It will provide advice on acceptable and effective control measures to enable children, young people and adults to use ICT resources in a safer online environment.

The policy applies to all individuals who are to have access to or be users of work-related ICT systems. This will include children and young people, parents and carers, Directors, early years Manager, Deputies, Educators, volunteers, students, visitors and contractors. This list is not exhaustive.

This policy will apply to internet access through any medium, for example computers, mobile phones and tablets. Before the use of any new technologies, they will be examined to determine potential learning and development opportunities and any restrictions put in place. Their use will be risk assessed before considering whether they are appropriate for use by children and young people.

Responsibilities

The Designated Safeguarding Lead (DSL) is to be responsible for online safety and will manage the implementation of this policy. In our setting the DSL is Ellie Green.

The Designated Safeguarding Lead will ensure:

- Day to day responsibility for online safety issues and will have a leading role in implementing, monitoring and reviewing this policy.
- All ICT users are made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.
- Recording, reporting, monitoring and filing of reports should a potentially unsafe and inappropriate incident occur.
- All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings take place with the Director (Clare) and Manager to discuss current issues and review incident reports.
- Effective training and online safety advice are delivered and available to the early year's Manager and Educators, including advisory support to children, young people, parents and carers as necessary for example the use of 'Think you Know' website.
- Liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Managing online access

Password security

- Maintaining password security is an essential requirement for early years Manager, Deputies and Educators particularly where they are to have access to sensitive information. A list of all authorised ICT users and level of access is to be maintained and access to sensitive data is to be restricted.
- All laptops/tablets should be set to 'timeout' the current user session should they become idle for an identified period.
- All ICT users must 'log out' of their accounts should they need to leave a laptop unattended, this is regarding office equipment.
- If ICT users become aware that password security has been compromised or shared, either intentionally or unintentionally, the concern must be reported to the Designated Safeguarding Lead
- Staff have access to individual tablets for children's online learning journeys. These are password protected and the Director (Clare) has access to all of these. A level of access is to be maintained and access to sensitive and personal data is to be restricted, only Director (Clare) Manager and Deputies having access and clearance for this data and information.

Internet access

- The internet access for all users will be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution will be taken to ensure the safe use of the internet. However, it must be recognised that it is impossible to safeguard against every eventuality.
- The following control measures will be implemented which will manage internet access and minimise risk:

  Secure broadband and wireless access
  A secure, filtered, managed internet service provider and/or learning platform

Secure email accounts
Regularly monitored and updated anti-virus protection
A secure password system
An agreed list of assigned authorised users with controlled access
Effective audit, monitoring and review procedures.

- Online activity is monitored to ensure access is given to appropriate materials only. Computers, laptops and tablets are sited in areas of high visibility to ensure children, young people and adults are closely supervised and their online use appropriately monitored. The Director (Clare) clears the history regularly on the her office laptop, the Manager (Ellie) will do the same and Educators will do their own devices.
- Should children, young people or adults discover potentially unsafe or inappropriate material, they must hide the content from view. N.B Children will not have access to the I Pad without Educator supervision and all IPADS and laptops has parental controls in place. Staff tablets are always out of reach. For example, the window will be minimised and/or the monitor (not computer) will be turned off. All such incidents must be reported to the DSL who must ensure a report of the incident is made and take any further actions necessary.
- Manager, Deputies and Educators will be made aware of the risk of compromising security, for example from connecting personal mobile devices to work related ICT systems. Such use is avoided but should it, on occasion be unavoidable it will be subject to explicit authorisation of the Designated Safeguarding Lead. Such use will be stringently monitored.
- Should it be necessary to download unknown files or programmes from the internet to any work-related system it will only be actioned by authorised ICT users with permission from the Designated Safeguarding Lead (DSL). Such use will be effectively managed and monitored.
- All users are responsible for reporting any concerns encountered using online technologies to the DSL.

Online communications

- All official communications must occur through secure filtered email accounts.
- All email and correspondence through Connect Childcare will be subject to scrutiny and monitoring.
- All ICT users are expected to write online communications in a professional, polite, respectful and non-abusive manner. The use of emojis is not permitted.
- A filtered internet server is used to monitor and prevent offensive material or spam. Should, on occasions, security systems not be able to identify and remove such materials the incident will be reported to the Designated Safeguarding Lead immediately.
- Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Early years Manager, Deputies and Educators will not share any personal information with any child or young person associated with the setting. They will not request or respond to any personal information from the child or young person other than which might be considered appropriate as part of their professional role. Advice should be sought from the DSL before engaging in any such communication.

- Early years Manager, Deputies and Educators must ensure that all communications are transparent and open to scrutiny. .
- Online communication is not considered private or confidential for safeguarding and security purposes. All users must seek advice from the DSL and the local Multi Agency Resilience and Safeguarding Board as to how information should be relayed.
- Children will be shown content from the internet, such as YouTube, only if it is deemed age appropriate. (Educators will view the content beforehand)
  .

Managing multimedia technologies

- Many devices are equipped with internet access, GPS, cameras and video and audio recording functions. A risk assessment is completed to minimise risk of using technologies whilst maximising the opportunities for children to access such resources.
- Access to a range of age-appropriate websites is available. Children are advised, in an age-appropriate manner, that they should be careful whilst online and that not everyone is who they say they are. The children are also spoken to about why we have passwords.
- All ICT users and the DSL must only use moderated sites to afford maximum protection. Non-moderated websites allow for content to be added and removed by others.
- Children will not be permitted to post images on any websites or profile.
- All photographs on computers and tablets are deleted termly.

Social networking sites

- Early years Manager, Deputies and Educators are not permitted to use work related technologies for personal access to networking sites.
- The use of these sites in adults recreational time cannot be restricted however early years Manager, Deputies and Educators must adhere to our professional conduct agreement. Content which may compromise professional integrity or will bring the setting into disrepute is not permissible and may result in disciplinary action – see staff handbook.
- It is not permissible for early years Manager, Deputies or Educators to engage in personal online communications with children, young people, parents or carers. This includes the use of social media networking platforms such as Facebook and Twitter and any other social networking site.
- Any known misuse, negative and/or anti-social practices must be reported immediately to the DSL

References to other relevant policies:

- Communication & Working in Partnership
- Confidentiality
- Image Use
- Safeguarding Policy and Procedures

Also see employee handbook

Policy Review

This policy is in line with the EYFS (DfE 2024)

This policy has been adopted by Bottesford Bunnies at staff meeting May 24th, 2018

Signed on behalf of the setting by:

……..Director

Next review date May 2019
Reviewed and updated at staff meeting May 2nd, 2019
Next review date May 2020
Reviewed and updated at staff meeting November 23rd, 2020
Next review date November 2021
Reviewed and updated at staff meeting October 2021 by Director, Manager, Deputy and practitioners.
Next review date October 2022
Reviewed and updated at staff meeting
Reviewed and updated at staff meeting 28th September 2022 by Director, Manager, Deputies and practitioners.
Next review date September 2023
Reviewed and updated at staff meeting 19th September 2023 by Director, manger, Deputies and educators,
Next review date September 2024
Updated February 11th, 2024, re changes to EYFS
Reviewed and updated at staff meeting October 2nd, 2024, by Director, Manager, Deputies and Educators
Next review date October 2025