Chudleigh Pre-school

Registered Charity No: 1028874   PLA No: 22478

Use of Internet Policy

1 Introduction

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

Children will learn most effectively where they are to be given managed access to ICT and control of their own learning experiences; however such use will carry an element of risk. Pre-school staff, alongside parents and carers, should consider it to be their duty to make children aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

2 Aim

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

3 Scope

The Internet Policy will apply to all individuals who are to have access to and/or be users of work-related ICT systems. This will include children, parents and carers, pre-school staff, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The Internet Policy will apply to internet access through any medium, for example, computers, mobile phones and tablets.

4 Responsibilities

The Designated Safeguarding Leads (DSLs) (Linda Palmer and Rachel Evans) are to be responsible for online safety, and will manage the implementation of the Internet Policy.

The DSL will ensure:

• day to day responsibility for online safety issues, and as such will have a leading role in implementing, monitoring and reviewing the Internet Policy.

• all ICT users are to be made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.

• receipt, recording, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. This must include the creation of an incident log to be used to inform future online safety practice.

• all necessary actions will be taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.

• regular meetings are to take place with the registered person (the committee) to discuss current issues, review incident reports and filtering/change control logs.

• effective training and online safety advice is to be delivered and available to all pre-school staff, as appropriate. This should include advisory support to children, parents and carers as necessary.

• timely liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Further details on the responsibilities of the DSL, the committee, pre-school staff, parents and carers and children are to be found in the Acceptable Use Policy.

5 Managing online access
Password security

Maintaining password security is to be an essential requirement for pre-school staff particularly where they are to have access to sensitive information. A list of authorised

ICT users is to be maintained, and access to sensitive and personal data is to be restricted.

Pre-school staff will be responsible for keeping their passwords secure and must ensure they are to be regularly up-dated. All ICT users must have strong passwords as defined by current government advice www.cyberaware.go.uk/passwords. Sharing passwords is not to be considered secure practice.

It is to be considered good practice for computers, laptops and tablets to 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 computer unattended.

If ICT users should become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the DSL.

Internet access

It is to be considered essential practice that internet access for all ICT 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. It has to be acknowledged however, that it will be impossible to safeguard against every eventuality.

The following control measures will be put in place which will manage internet access and minimise risk:
- Secure broadband or wireless access.
- A secure, filtered, managed internet service provider.
- Secure email accounts. Where confidential information is to be exchanged (for example, regarding Safeguarding or SEN issues) emails will be sent using Egress Switch.
- Regularly monitored and updated virus protection.
- A secure password system.

- An agreed list of assigned authorised users with controlled access.
- Clear Acceptable Use Policies and Agreements.
- Effective audit, monitoring and review procedures.
- The childrens' tablets (Kindle Fire for Kids) are set up with parental controls so that only content suitable for 2-4 year olds may be viewed. The adult mode (which is the only means by which apps, books and films can be downloaded) is password protected.

Online activity is to be monitored to ensure access will be given to appropriate materials only.

Computers and tablets accessible to children are to be sited in areas of high visibility which will enable children and adults to be closely supervised and their online use to be appropriately monitored.

Should children or adults discover any potentially unsafe or inappropriate material, they are to hide the content from view. For example, the window will be minimised and/or the monitor (not computer) will be turned off. The use of the CEOP Hectors World browser button and Report Abuse button are to be considered best practice[1]. All such incidents must be reported to the DSL who must ensure a report of the incident is to be made and will take any further actions which are to be deemed necessary.

[1] Child and Exploitation Online Protection Centre – free to all settings and available from www.thinkuknow.co.uk

All staff are to be made aware of the risks of compromising security, for example from connecting personal mobile devices to work-related ICT systems. Such use is to be avoided as far as is practically possible. Should, on occasion it be unavoidable, it will be subject to explicit authorisation by the DSL. Such use will be stringently monitored.

Should it be necessary to download unknown files or programmes to any work-related system, it will only be actioned by authorised ICT users with express permission from the DSL. All such use will be effectively managed and monitored.

All users are to be responsible for reporting any concerns encountered using online

technologies to the DSL.

Online communications
Emails

All official online communications containing personal data must occur through secure filtered email accounts with the additional use of Egress Switch recommended, particularly with regards to official communications regarding Safeguarding or SEN. Web-based commercial email services are not to be considered secure. We share official reports (Transition Documents, 2 Year Progress checks) to a secure online sharing platform for printing.

All email correspondence may be subject to scrutiny and monitoring.

All ICT users will be expected to write online communications in a polite, respectful and non-abusive manner. The appropriate use of emoticons is to be encouraged.

A filtered internet server is to be used to monitor and prevent offensive material or spam. Should, on rare occasions, security systems not be able to identify and remove such materials, the incident will be reported to the DSL immediately.

In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'[2] it will not be considered appropriate for early years practitioners or their managers to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites under Principle Eight of the GTC Code of Practice[3].

[2] http://www.safeguardinginschools.co.uk/guidance-for-safer-working-practice-for-adults-who-work-with-children-and-young-people-in-education-settings/

[3] General Teaching Council 'Demonstrate honesty and integrity and uphold public trust and confidence in the teaching profession'.

5.3.6 Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Pre-school staff should not share any personal information with any child or young person associated with the early years setting. They should not request or respond to any personal information

from the child other than that might be considered appropriate as part of their professional role. Early years practitioners and their managers should ensure that all communications are to be transparent and open to scrutiny.

All ICT users are to be advised not to open emails where they do not know the sender or where the format looks suspicious.

Online communication is not to be considered private or confidential for safeguarding and security purposes. Such communication is to be monitored and must be available for scrutiny at any time.

Children will be enabled to use online equipment and resources, when it is to be considered, in consultation with parents and carers, that they have the developmental knowledge and understanding to recognise some of the benefits and risks of such communication. Access to online communications will always be monitored by a supervising adult.

Social Media
Chudleigh Pre-School has a Facebook page that is used to communicate with parents and carers for the following purposes:
- information about themes and topics the pre-school is following week by week
- information about events
- information about session changes, new sessions opening etc.
- reminders for parents/carers
- photographs of craft activities etc. that the children have made

The Facebook page will not contain
- names of pre-school staff, children or committee
- pictures of children at pre-school
- pictures of staff without their consent
- information pertaining to any individual(s) linked to the pre-school in any way.

It is to be recognised that pre-school staff are likely to use social networking sites in their recreational time on their own personal devices. This form of activity is not to be discouraged, however all pre-school staff must agree and adhere to a 'professional conduct agreement'. It must be ensured that the use of such sites will not compromise professional integrity or bring the early years setting into disrepute. The adding of children and young people, parents and carers as 'friends' to a social networking site should be avoided.

Children, parents and carers are to be informed that the use of social networking sites in the home or social environment is to be seen as an exciting communication and networking tool. It must also be emphasised however that their use can pose potential risks. Children, parents and carers should therefore be made aware of the potential risks, and the control measures that can be implemented to minimise them.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbulling, for example, is to be considered as unacceptable as any other form of bullying and effective sanctions must be in place to deal with such concerns. Any known or suspected incidents must be reported immediately to the DSL.

Managing multimedia technologies

For practical purposes, multimedia technologies at Chudleigh Pre-School refers to the use of tablets, both by adults and children within the setting. Multimedia technologies, where they are to be used responsibly, will provide easy to use, creative, collaborative and free facilities. However, it is to be recognised that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

These technologies should be valued for the learning and development opportunities they will provide for children and young people; including a move towards personalised learning and one to one device ownership. Many existing technologies such as portable media players, gaming devices, tablets and mobile phones will already be familiar to many children.

These devices will invariably be equipped with internet access, GPS, cameras, video and audio recording functions. They should therefore be considered subject to the same risks as any other form of technology. Effective control measures should therefore be put in place to minimise such risk whilst maximising the opportunities for children and young people to access such resources.

Access to a range of age appropriate websites should be enabled, but children should be encouraged to be cautious about any information given to them by other users on such sites, and must recognise that not everyone is who they say they are.

Use by Children:

Access to a range of age appropriate apps should be enabled, and the opportunity to look at carefully filtered websites under the direction of an adult is permitted. Children should be taught age appropriate principals of online safety.

- Only go online with a grown-up
- Be kind on line
- Keep information about me safely
- Only press buttons on the internet to things I understand
- Tell a grown up if something makes me unhappy on the internet.

Use by adults:

An online Learning Journey called Tapestry is used by Chudleigh Pre-School. Staff must adhere to the guidance provided with the system, refer to relevant training and all ICT policies at all times. Parents / carers given access to the system must abide by the ICT policies, with particular with regards to the Camera and Image Policy.

Access to social networking sites is not permitted within the setting. In addition, Pre-school staff are not permitted to use work-related technologies for personal access to social networking sites.

.

Emerging technologies

Emerging technologies are to be examined to determine potential learning and development opportunities. Their use is to be risk assessed before consideration will be given to enabling use by children. Where necessary, further training and guidance is to be sought to ensure appropriate and safe use of any new technologies.

Adopted at Committee Meeting

24 May 2012

Reviewed July 2013, September 2014, October 2017, September 2021

Related Policies:

Acceptable Use Policy

ICT Misuse Policy

Camera and Image Policy

Mobile Technology Policy

Safeguarding Children and Looked After Children Policy

Confidentiality and Data Protection Policy