Online Safety
Internet Policy

1 Introduction

1.1 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 and young people's enjoyment of learning and development.

1.2 Children and young people will learn most effectively where they are to be given managed access to computers and control of their own learning experiences; however, such use will carry an element of risk. Early years practitioners and their managers, alongside parents and carers, should consider it to be 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 safe, without limiting their learning opportunities and experiences.

2 Aim

2.1 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

3.1 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 and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

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

4 Responsibilities

4.1 The Senior Designated Person for Safeguarding (SDPS) is to be responsible for online safety, and will manage the implementation of the Internet Policy.

4.2 The Senior Designated Person for Safeguarding 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 and senior managers 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 early years practitioners and their managers. This should include advisory support to children, young people, 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.

4.3 Further details on the responsibilities of the Senior Designated Person for Safeguarding, registered person, early years practitioners and their managers, parents and carers, children and young people are to be found in the Acceptable Use Policy.

5 Managing online access

5.1 Password security

5.1.1 Maintaining password security is to be an essential requirement for early years practitioners and their managers 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.

5.1.2 Early years practitioners and their managers will be responsible for keeping their passwords secure and must ensure they are to be regularly up-dated – at least once every 60 days. All ICT users must have strong passwords, for example, an impersonal combination of numbers, symbols and lower/upper case letters.

5.1.3 Sharing passwords is not to be considered secure practice. Where children and young people are to be enabled to create their own password however, a copy of such will be kept on file for reference.

5.1.4 It is to be considered good practice for computers and laptops 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.

5.1.5 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 Senior Designated Person for Safeguarding.

5.2 Internet access

5.2.1 I t 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.

5.2.2 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 and/ or learning platform.
- Secure email accounts.
- 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.

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

5.2.4 Computers and gaming machines are to be sited in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.

5.2.5 Should children, young people 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 Senior Designated Person for Safeguarding; who must ensure a report of the incident is to be made and will take any further actions which are to be deemed necessary.

5.2.6 All early years practitioners and their managers 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 Senior Designated Person for Safeguarding. Such use will be stringently monitored.

5.2.7 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 Senior Designated Person for Safeguarding. All such use will be effectively managed and monitored.

5.2.8 All users are to be responsible for reporting any concerns encountered using online technologies to the Senior Designated Person for Safeguarding.

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

5.3 Online communications

5.3.1 All official online communications must occur through secure filtered email accounts. Web-based commercial email services are not to be considered secure.

5.3.2 All email correspondence will be subject to scrutiny and monitoring.

5.3.3 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.

5.3.4 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 Senior Designated Person for Safeguarding immediately.

5.3.5 In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'[1] 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[2].

5.3.6 Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Early years practitioners and their managers 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 or young person 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.

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

5.3.8 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.

5.3.9 Children and young people 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.

5.4 Managing multimedia technologies (including Web2 and 3G technologies)[3]

5.4.1 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.

5.4.2 Emerging 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

[1] http://www.dcsf.gov.uk/everychildmatters/ resources-and-practice/IG00311/

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

[3] Web 2–second generation of web communications (for example, social networking sites). 3G–next generation of mobile/wireless technologies.

existing technologies such as portable media players, gaming devices, and mobile phones will already be familiar to many children and young people.

5.4.3 Many of these devices will 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.

5.4.4 Access to a range of age appropriate websites should be enabled, but children and young people 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.

5.4.5 Access to social networking sites and online chat will not be permitted within the early years setting, and children and young people will only be permitted to use moderated child-focused sites under supervision. Early years practitioners and their managers are not permitted to use work-related technologies for personal access to social networking sites.

5.4.6 All ICT users are to be encouraged to think carefully about the way information can be added and removed from websites by themselves and others. Moderated sites, through SWGfL, such as 'Learning Platform Merlin' and 'My First Place' are therefore to be used to afford maximum protection.

5.4.7 Children and young people will be taught to think carefully before placing images of themselves on such sites and to be aware of details within images, such as a school badge, which could reveal personal and background information. Children and young people should consider the appropriateness of any images owing to the permanency of online material.

5.4.8 Children and young people must always be reminded not to give out or post personal details on websites, particularly information which could identify them or provide information that would contribute to their personal profile. For example, full name, address, mobile/home telephone numbers, school details, IM/email address and specific hobbies/interests.

5.4.9 Children and young people are to be advised on how to set and maintain web profiles to appropriate privacy levels and to deny access to unknown individuals.

5.4.10 Children and young people, 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 and young people, parents and carers should therefore be made aware of the potential risks, and the control measures that can be implemented to minimise them.

5.4.11 I t is to be recognised that early years practitioners and their managers are also likely to use social networking sites in their recreational time on their own personal computers. This form of activity is not to be discouraged however early years practitioners 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.

5.4.12 It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbullying 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 Senior Designated Person for Safeguarding.

5.5 Emerging technologies

5.5.1 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 and young people. Where necessary, further training and guidance is to be sought to ensure appropriate and safe use of any new technologies.

6 Authorisation and review

This policy was adopted at a meeting of	Wroughton Preschool
Held on	
Date to be reviewed	Yearly at AGM
Signed on behalf of the management committee	
Name of signatory	
Role of signatory (e.g. chair/owner)	Chairperson