Online Safety
A Toolkit for Early Years Settings

Social Care document type
Toolkit

Title
Online Safety: A Toolkit for Early Years Settings

Document purpose and description
This toolkit will aim to highlight and endorse best practice for managing the risks associated with online technologies. Included are policies and procedures which are to be used as exemplars. This means they should be considered best practice. Early years settings will be required to tailor the policies to meet their own individual requirements, but there is to be an expectation that the core messages and values will remain.

Author(s)/editor(s)
Maria Hollett, Tony Staunton, Ken Corish, Viv Venn.

Endorsed by
Bronwen Lacey and Councillor Grant Monahan

Endorsement date
31 March 2010

Publication date
28 April 2010

Review date
28 April 2011

Job title of person responsible for review
Maria Hollett
Early Years Development and Childcare Co-ordinator

Target audience
Early years and childcare settings, childminders and children’s centres.

Circulation list
Early years and childcare settings, childminders and children’s centres.

References
Please see Appendix 1

Supersedes document
Version 1

Contact details
Early Years Team (All Children First)
Services for Children and Young People, Plymouth City Council
Plymouth PL1 2AA
Telephone: (01752) 307450
Email: earlyyears@plymouth.gov.uk
Online Safety: A Toolkit for Early Years Settings is designed to be used by a range of organisations, including nurseries, pre-schools, out of school clubs, crèches, childminders and children’s centres. The toolkit primarily aims to inform services provided for the early years age group (birth to five years), but the core messages will also apply to any organisation working with older children and young people. Online safety is to be recognised as both a philosophy and a statutory requirement. It is to be defined not only by policy but also by leadership, infrastructure, education, monitoring and review. This wider view will lead to the cultural changes needed to support online safety in practice. This toolkit will aim to highlight and endorse best practice for managing the risks associated with online technologies. Included are policies and procedures which are to be used as exemplars.

These comprise of:
- a primary Acceptable Use Policy.
- four other sub policies.

These policies are to be considered best practice. The Acceptable Use Policy should be deemed the absolute minimum that any early years setting should adopt as a baseline requirement. Early years settings will be required to tailor the policies to meet their own individual requirements, but there is to be an expectation that the core messages and values will remain. It should be noted that the policies are designed to be generic and as such will apply to a range of early years settings who offer distinct types of care and work with children of various ages. It should therefore be recognised that not all aspects of each policy will be applicable or relevant to all organisations.

"Safety needs careful thought and discussion to arrive at decisions that are balanced, fair and effective."
The Royal Society for the Prevention of Accidents

\(^1\) The term ‘early years setting’ will be used throughout the document for ease of reference. It should be taken as referring to nurseries, pre-schools, out of school clubs, crèches, childminders and children’s centres.

\(^2\) N.B. There is a whole range of appropriate model policies for other education and social care settings available and freely adaptable from the South West Grid for Learning.
Contents

4 Foreword

7 Chapter 1: Introduction to Online Safety in Early Years Settings
  7 Section 1 Introduction
  10 Section 2 Online Safety
  15 Section 3 Policies and Practice
  16 Section 4 What is an AUP?
  18 Section 5 Useful Information and Contacts

21 Chapter 2: Acceptable Use Policy (AUP)

31 Chapter 3: Internet Policy

39 Chapter 4: Camera and Image Policy

59 Chapter 5: Mobile Phone Policy

67 Chapter 6: ICT Misuse Policy

73 Appendices
  75 Appendix 1 References
  76 Appendix 2 The Risks Associated with ICT - FAQs
  79 Appendix 3 Plymouth Interagency E-safety Pledge
  81 Appendix 4 Image Consent Letter
  83 Appendix 5 Consent Form for Taking Images
  85 Appendix 6 Group Activity Permission Letter and Form
  87 Appendix 7 Online Safety Acceptable Use Agreement
  89 Appendix 8 Online Incident Log Sheet
  91 Appendix 9 Online Safety Incident Log
  92 Appendix 10 Consent to Use an Image Form
  93 Appendix 11 Photography Consent Form
  94 Appendix 12 Professional Conduct Agreement
  95 Appendix 13 Acceptable Use Rules for Children
  96 Appendix 14 Learning Journey Trust Statement
  97 Appendix 15 Learning Journey Consent Form
  98 Appendix 16 Key Principles for the Safe Use of ICT in Early Years
Dear Colleague,
The online world is upon us, bringing with it an array of feelings ranging from caution and doubt through to excitement and fascination. The one consistent factor is that the online world is here to stay. Newer and more advanced technologies are developing and evolving everyday bringing with them an exciting culture which we need to embrace.

We have, through the online world, tremendous opportunities to learn, to be creative and to communicate with each other globally, through both work and play. We could never have dreamt when we were young, the wealth of information and knowledge we would have at our fingertips as adults.

Today, however, our children and young people are growing up with these new technologies. They have become an integral part of our children’s daily lives; and whereas we may sometimes find it hard to grasp new concepts and opportunities, the young are grabbing them by the hand and enthusiastically seeking newer, faster and more accessible versions.

The very fact that our children and young people are so keen to grasp every opportunity and to embrace the new and unfamiliar naturally makes us cautious. We are the adults. We are the ones who are supposed to have the knowledge. Increasingly, however, our children and young people are becoming the experts in this field. How, therefore, can we protect and safeguard our children and young people, when we don’t have a clear understanding ourselves of the available technologies and the potential risks?

This is the critical point: why it is so crucial to understand online safety, not only to give us as adults the knowledge to keep children and young people safe, but also to help us equip them with the skills and the resilience to recognise and address risk.

This guide is designed to increase awareness and understanding of online safety; the knowledge behind the policies; the understanding of why certain procedures must be carried out; the acceptance of the potential risks and the empowerment and resilience to recognise, avoid and report dangers before they have the opportunity to escalate.

The knowledge and understanding to be gained will give us the opportunity and confidence to join our children and young people in embracing this new online culture; allowing them to flourish and grow by reaping all the benefits of such exciting developments. It is only by embracing this culture that we can be confident and reassured that our children and young people have the skills and knowledge to understand the difference between acceptable use and misuse; and the empowerment and resilience to keep safe. In the same way that safeguarding is everybody’s business; online safety is everybody’s business. We must learn together.

Bronwen Lacey
Director of Services for Children and Young People

Councillor Grant Monahan
Cabinet Member for Children and Young People

31 March 2010.
Chapter 1
Introduction to Online Safety in Early Years Settings
“Whatever you’re born with is “normal”. Anything that gets invented after you’re 30 is against the natural order of things and the end of civilisation as we know it...until it’s been around for 10 years or so.”

Douglas Adams
Section 1: Introduction

1.1 Technology has developed over recent years and will continue to evolve, leaving many of us struggling to keep up. Children and young people will often be the first to embrace new technologies. As an adult it can be daunting to embrace a culture which requires us to fully understand a wide range of developing technologies that we have not been brought up with.

1.2 Information and communication technology (ICT) has had, and will continue to have, a profound effect on the way we communicate. For example, texting, instant messaging and emailing are to be considered for many a normal and accepted means of ‘written’ communication.

1.3 ICT encompasses a wide range of media applications and connecting methods, which are continually changing and advancing. These include:
- Computers and laptops – access to fixed and mobile internet, email, chat rooms, blogs, social networking sites, podcasts, instant messaging and location based technologies like Latitude and GPS;
- Wireless and Broadband access;
- Mobile phones with internet access, Bluetooth, cameras, videos, WiFi and more;
- Gaming – online and game consoles, such as the Wii or PSPs, many of which can interconnect with other devices;
- Video broadcasting and music downloading;
- Digital cameras;
- Whiteboards.

1.4 We cannot stop advances in technology and nor should we try to do so. We should not prevent any member of our learning community from having access to such enabling resources - to do so would border on social exclusion and could potentially infringe on human rights. It is to be recognised that children and young people have rights as learners. They should be entitled to have access to the most appropriate technologies to support their learning and development to prepare them for the ‘real’ world.
The role of ICT in learning and development

1.5 Early years practitioners and their managers are to be encouraged to recognise the exciting opportunities and the innovative tools advances in technology will provide. This should be deemed central to their role of supporting the learning and development needs of children and young people. It must therefore be considered vital that early years practitioners and their managers will have a clear and agreed understanding of the benefits and risks of such technology.

1.6 Sir Jim Rose, in his review of primary education, is to emphasise ‘that used well, technology strongly develops the study and learning skills children and young people need now and in the future, including the fundamentals of e-safety’.

1.7 The influence and value of ICT should be seen as firmly embedded within the Early Years Foundation Stage and it must therefore be reflected in practice. It is to be anticipated that by the end of the Foundation Stage, most children will be able to demonstrate and achieve the following early learning goal: ‘Find out about and identify the uses of everyday technology and use information technology and programmable toys to support their learning’.

1.8 To reflect this, early years practitioners and their managers should be encouraged to ‘support children and young people in using a range of ICT [resources] to include cameras, photocopiers, CD players, tape recorders and programmable toys in addition to computers’. Early years practitioners and their managers should also be able to support children and young people to ‘talk about ICT apparatus, what it does, what they can do with it and how to use it safely’.

1.9 The indirect, as well as the direct, impact of ICT on children and young people’s learning and development should also be considered. Early years practitioners and their managers should be expected to use a range of technological resources to manage their roles as professionals; to be enabled to use the internet to research and communicate professionally; to use online systems to track and record the progress of children and young people and to share their work; to communicate with parents and carers through newsletters, email or

---

1 The term ‘early years practitioner’ will be used throughout this document for ease of reference. It should be taken as referring to any individual working with children, including qualified and unqualified staff, volunteers and students.


3 Early Years Foundation Stage - (Knowledge and Understanding of the World) DCSF 2008.

4 Early Years Foundation Stage - DCSF 2008.
the internet and to be able to manage administrative tasks and systems. All of these should be referenced as areas that require clear agreements regarding acceptable use; and must be recognised for their indirect value in supporting the learning and development of children and young people.

1.10 Many children and young people will have their own language exclusive to the online world, and will use abbreviations like LOL (laugh out loud) and symbols, such as emoticons. This use of language will often make adults feel unqualified and out of their depth. Children and young people themselves will also feel, and be, socially excluded should they not be given the same opportunities to access the wide range of technologies as their peers. It must therefore be considered essential to the lifelong learning experiences of children, young people and adults that the online world is to be fully embraced. This should include a recognition and acceptance of both benefit and risk.

1.11 The dilemma for many early years practitioners and their managers will often be that they will put various control measures in place without entirely understanding the rationale for doing so. Imparting individuals with online safety knowledge must therefore be considered an essential first step towards ensuring policies and procedures are to be realistic, manageable and able to be implemented in practice. If the reason and rationale for doing something is to be understood, it should be more likely that such practice will be adopted.

1.12 Learning about technology will increasingly be seen as an essential life skill that all children and young people should be aware of, understand and feel empowered to use efficiently and safely. The importance of up-to-date high quality online safety training and support for early years practitioners and their managers must therefore be considered paramount.

1.13 Early years settings must take responsibility for providing online safety guidance and education to children and young people. This will promote safer use of online technologies both within the setting and home environment. Children and young people should learn how to moderate their own behaviours, but must also be enabled to recognise inappropriate behaviour in other users.

“Practitioners will support children in using ICT resources appropriately, helping them to make sense of the world around them in a range of real situations.”

Jo Paterson, Early Years Regional Advisor, South West, The National Strategy
What is online safety?

2.1 The term ‘online safety’ is to be used to encompass the safe use of all forms of information and communication technologies. The aim, through online safety, should be to reasonably protect all users of such technologies from potential and known risk. Technology itself is to be seen as only one aspect of this; equally as important are the ways in which technology and behaviours will be managed. For safeguarding to be effective, online safety procedures must be clear, agreed and respected by everyone.

2.2 Online safety practice will involve valuing the opportunities offered through information and communication technologies (ICT), recognising potential risks and understanding and implementing the control measures that need to be put in place to reduce them.

2.3 Effective online safety practice will enable children and young people to use technology safely, whether at home, in the early years setting or within the social environment. It will empower them to use their acquired skills and knowledge to keep themselves safe, without limiting opportunities for exploration, creativity and innovation.

2.4 Current research will demonstrate that managing risks around technology will provide a better learning experience for children and young people. As is to be evidenced in the recent Ofsted report ‘Safe use of new technologies’5 ‘locked down’ practices are not to provide effective safeguards. Prohibiting access to online technology within early years settings is to give a false sense of security. Adults may feel safer, but children and young people are to be more vulnerable as they will not be empowered with the knowledge and skills to keep safe. The online world is to be part of our culture, and the fact that it is to include both benefit and risk must be recognised.

2.5 It should be recognised that the online world is here to stay. This will invariably lead to a level of concern and risk. Online technology is to create a form of communication which is ‘permanent, traceable, and accessible to anyone with the knowledge and power to open it’6. It must therefore be handled with caution and care. Individuals must however endeavour to recognise the whole picture, and appreciate that fundamentally the main risks should not be related to a piece of equipment, but to the behaviours of the individuals using it.

---

5 www.ofsted.gov.uk
6 Safeguarding Cyberworld, Tony Staunton, Plymouth Safeguarding Children and Young People’s Board (2009).
2.6 Universal efforts should be concentrated on minimising risk, whilst empowering children, young people and adults to recognise the potential hazards and signs of online misuse. This will build resilience and the ability to make informed, measured judgments and decisions regarding acceptable use. It is to be unrealistic and naïve to feel that all risks are to be eliminated.

2.7 Tanya Byron, in the report ‘Safer Children and Young People in a Digital World’ is to highlight three strategic objectives which should be considered when determining the safety of children and young people accessing the internet. These objectives will be to ‘reduce availability, restrict access and increase resilience’, and as such are to be considered when developing policies and procedures to promoting online safety. The result of which should improve children and young people’s knowledge and understanding; will build their resilience and empower them to use online technologies in a safer, more responsible and effective way.

What are the risks?

2.8 The difficulty with online safety is that individuals will frequently be afraid to acknowledge risk; it may make people feel uncomfortable or overwhelmed, and it will often be felt that it is simply easier to ‘ban’ certain aspects of use. Alternatively, people may feel the risk is so small that it will never happen, and will therefore fail to put sufficient procedures in place. The aim should be to create a balance.

2.9 It must be appreciated that safeguarding is everybody’s business and therefore the paramount concern will be to ensure the safety and wellbeing of children and young people. This is to include their online safety.

2.10 The risks that must be addressed and managed through online safety will often be similar to those experienced in the ‘real’ world. Safeguarding practice should, therefore, acknowledge that both ‘real’ and ‘virtual’ worlds will essentially pose similar risks, challenges and dilemmas. For example, cyber bullying, and physical bullying should both be taken as seriously as each other. The physical effects may well be different, but the emotional effects will often be similar. Consistent consequences and sanctions for such should therefore be applied.

7 Tanya Byron ‘Safer Children and Young People in a Digital World’ 2008 www.dcsf.gov.uk
2.11 With an unsecured online environment in particular, it must be remembered that it is a public place. Information shared online on unsecured sites will be held in the public domain, and therefore precautions we are to adopt in our ‘real’ life situations should be transposable.

2.12 It must also be recognised that there will be significant implications around data security should unsecured sites be used. This will include how personal data is to be held and processed and who will have access to it. The sole use of secure sites is therefore to be recommended; as they will give additional protection by ensuring personal information is not available to the general public.

2.13 As with any form of safeguarding, the potential risks to children and young people must therefore be recognised. These are to include the potential risks from:

- prolonged exposure to online technologies, particularly from an early age.
- exposure to inappropriate content, images and language.
- making, taking and distribution of indecent images and ‘sexting’.
- cyber bullying.
- grooming.
- physical, sexual and emotional abuse.
- addiction to gambling and/or gaming.
- pressure from media and targeted advertising.
- theft and fraud from activities such as phishing.
- viruses, Trojans, diallers, key loggers, spyware and other malware.
- social pressure to maintain online networks via texting and social networking sites.
- identity theft.

**Managing the risk**

2.14 Demonstrating how risk will be managed, and how all ‘reasonable’ precautions will be taken to protect users should be essential practice for all early years settings. Early years settings, who are to be recognised as delivering best practice will have clear and effective policies, practices and infrastructure in place; which will be monitored and regularly reviewed to ensure they will be able to continue to meet the ever-changing needs of their specific learning community.

2.15 In early years settings, the registered person will have the overall legal, personal and moral responsibility to ensure online safety will be effectively considered. This means the registered person will not only be responsible for the safety of children and young people in their care, but also for the behaviours and expectations of any adults who affect or come into contact with the early years setting. This is to include a responsibility for monitoring the behaviours of all early years practitioners and their managers, parents and carers, visitors and contractors. This list should not be considered exhaustive.

---

8 malicious software and viruses.
9 The term ‘registered person’ will be used throughout the document for ease of reference. It should be taken as referring to an individual or organisation which is registered with Ofsted to provide childcare. This is to include employers, individuals, private, voluntary and independent organisations, committees, trusts and governor-run provision.
2.16 The registered person will also have overall responsibility for ensuring online safety practice will be managed and implemented effectively, within the requirements of the law. This will often be complex and challenging. In reality, however, safeguarding should be considered everybody’s business and therefore an agreed, shared approach must be promoted by all.

2.17 Online safety should therefore not be seen as the sole responsibility of one individual. Effective training and awareness raising, reliable infrastructure and clear acceptable use agreements should be considered key to effective practice.

A safer online environment in early years settings

2.18 The registered person is to be responsible for applying a duty of care by creating a safer online environment for all users.

2.19 The process of creating and maintaining a safer online early years environment will be challenging and complex but will be achievable and empowering. It is to be recognised by all users that in order to create such an environment, it will require the need to:

- modify behaviours
- change procedures and practices
- provide support, guidance and training for all.

2.20 Creating a safer online environment will be ongoing and ever-changing and will, therefore, take time to fully introduce into everyday practice. Clear monitoring, evaluation and review procedures are to be essential elements for ensuring a safer online learning environment - which will be ready to meet the new challenges that advancing technology will continue to provide.

Equality of opportunity

2.21 All children, young people and adults will be encouraged to use and benefit from the opportunities provided by a range of ICT technologies.

2.22 It will be recognised, however, that some children and young people may require additional support and guidance. This may include reminders, prompts and further explanations to reinforce and develop each individual’s existing knowledge and understanding of online safety issues.

Parental involvement

2.23 It should be considered essential for parents and carers to be fully involved with promoting online safety within the setting, home and social environment. It will be advantageous therefore to regularly consult with and discuss online safety issues with parents and carers. The aim should be to encourage a broader understanding of the benefits and risks of ICT and to agree policies and procedures which define acceptable use.
2.24 Parents and carers should be encouraged to sign Acceptable Use Agreements on behalf of, and with, their children. This will encourage a shared understanding of acceptable use, and such agreements should therefore be developed in line with the Acceptable Use Policy.

2.25 Parent or carer permission must be obtained for taking and making photographs, video or audio recordings of children in the care of the early years setting. Consent should also be obtained for the subsequent use of any images or recordings made.

2.26 Best practice will be recognised where early years practitioners and their managers are seen to be working in close partnership with parents and carers. As such early years practitioners and their managers should provide assistance in directing parents and carers to the best sources of advice for information on the safe use of ICT in the home and/or social environment.
Section 3: Policies and Practice

3.1 A large proportion of issues surrounding online safety are to be linked to the behaviour of users – whether children, young people or adults. It should therefore be considered essential that online policies, procedures and practices are developed with the aim of modifying behaviours and promoting acceptable use. Clear sanctions should also be identified to deal with any incidents or allegations of potential misuse.

3.2 In order to be effective, policies and procedures must be rigorous, enforced, monitored and reviewed to ensure they are to remain fit for purpose.

Supporting resources to enable online safety within an early years setting

3.3 ‘PIES’\(^{10}\) should be recognised as a successful and best practice model which will enable the effective risk management of online safety practice. Following the PIES model will be a simple and effective way of minimising exposure to risk through:

- Policy and practice
- Infrastructure and technology
- Education and training
- Standards and inspection

3.4 The ‘360 Degree Safe’ model and the ‘Online Safety Planner’ developed by the South West Grid for Learning (SWGfL) are to be seen as powerful audit tools which should be recognised as best practice for reviewing online safety procedures. The tools will not only audit current provision, but will also benchmark progress; provide clear friendly advice on how to progress further; manage reports and help develop and identify future planning and training needs. The audit tools will be underpinned by supporting resources and will lead to accreditation through the SWGfL Online Safety Charter Mark. SWGfL will also provide a consultancy and assessment service to support those using the tool.

3.5 The Online Safety Planner in particular will be most beneficial for early years settings, as it has been specifically written for small organisations. It is a vital tool that should not be overlooked and can be found at www.360safe.org.uk

\(^{10}\)Becta PIES model to reduce the risks of online safety - www.becta.org.uk
Section 4: What is an Acceptable Use Policy (AUP)?

4.1 An AUP is a policy which will:

• identify that children and young people will learn most effectively where they are to be empowered to be safe and responsible users; and where they are to be enabled to make effective judgements about what they see, find and use.

• set out the roles, responsibilities and procedures which should govern the acceptable use of all online technologies with the aim of safeguarding children, young people and adults from harm.

• outline how training will be delivered to early years practitioners and their managers. This should also include how support and guidance will be provided (where appropriate) to parents, carers and the wider community to promote the safe and responsible use of online technologies.

• set out clear, concise guidelines for the acceptable use of information and communication technology (ICT). It will also identify how such guidelines will be monitored, evaluated and reviewed regularly to ensure they are to remain fit for purpose in light of changing technologies.

• be a means of agreeing, recording and communicating behaviours which are to be considered acceptable or unacceptable.

• outline the reporting procedures and sanctions which are to be implemented should ICT be intentionally or unintentionally misused by children, young people or adults.

• include clear statements, which should include monitoring strategies, so that all users will be aware that their behaviours, files and activities may be monitored. It should be evidenced how rigorous monitoring will ensure that standards through inspection will be maintained.

4.2 Fundamentally, AUPs and online safety guidelines should form an integral part of the welfare, learning and development programme for all children and young people. Effective links must therefore be made to key policies and procedures, such as safer recruitment, induction and safeguarding, and firmly embedded in PSED (personal, social and emotional development) activities.

---

11 Includes the internet, email, webcams, instant messaging and other social networking spaces, mobile phones, games and more.
Chapter 1: Introduction to Online Safety in Early Years Settings

4.3 There will always be risks when using any form of communication which lies within the public domain. It should therefore be considered essential that clear rules, procedures and guidelines will be in place to minimise those risks. It must, however, be recognised and accepted that it will be impossible to eliminate all risk completely.

4.4 Acceptable Use Policies are to be fundamental to risk management. The exemplar AUP and supporting sub-policies in isolation are to be considered a base line to minimising risk. In order to maximise impact however, it will be essential for all areas of policy, procedure and practice to link together to ensure clear, effective and joined up strategies are to be fully established and implemented.

4.5 Furthermore, it should be considered essential that early years practitioners and their managers have a clear understanding of what will be considered acceptable and unacceptable behaviours. This should help to ensure the behaviour of ICT users will not be open to misinterpretation or lead to allegations as a result of any individual’s lack of knowledge of the potential risks.

4.6 It will only be by ensuring all ICT users will have a clear understanding of acceptable and unacceptable use that behaviours will be effectively managed and modified. Subsequently, this will lead to a safer online learning environment for all.

4.7 As part of the Government’s Every Child Matters ‘Outcomes for children’ agenda and through the Children’s Act 1989 and 2004, it is considered to be everybody’s duty to ensure that children and young people will be protected from potential harm. The involvement of children, young people, parents and carers is to be considered vital to the effective and safer use of online technologies. The AUP should therefore inform children, young people, parents and carers of their own responsibilities. The process of developing an AUP should be consultative, taking account of the views of all those involved.
Section 5: Useful Information and Contacts

Plymouth City Council
Early Years Team (All Children First)
Services for Children and Young People
earlyyears@plymouth.gov.uk
(01752) 307450

SWGfL Staying Safe
http://www.swgfl.org.uk/Staying-Safe
Collection of advice, support and resources for early years practitioners and their managers, children and young people, parents and carers.

Childnet International
http://www.childnet-int.org/
Wide range of resources, in particular the acclaimed ‘Know IT All for Parents and Carers’.

CEOP
www.thinkuknow.co.uk
Child Exploitation and Online Protection Centre site with education resources from KS1 and Foundation.

The Byron Review
http://www.dcsf.gov.uk/byronreview/

Click Clever Click Safe
The first UK Child Internet Safety Strategy (UKCCIS UK Council for Child Internet Safety).

“Children’s brains work faster than adults’ brains. That’s why we’re better at using the technology.”
Child, Byron Progress Review 2010.
Chapter 2

Acceptable Use Policy (AUP)
“A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools.”

Douglas Adams
Chapter 2: Acceptable Use Policy (AUP)

1 Aim

1.1 The Acceptable Use Policy (AUP) will aim to:

- safeguard children and young people by promoting appropriate and acceptable use of information and communication technology (ICT).
- outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems.
- ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

2 Scope

2.1 The AUP 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.

2.2 Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where known, off-site.

3 Roles and responsibilities

3.1 Registered person

The registered person is to have overall responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice. This will include ensuring:

- early years practitioners and their managers will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- the AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- monitoring procedures are to be open and transparent.
- allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
• effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection.

3.2 Senior Designated Person for Safeguarding (SDPS)
The Senior Designated Person for Safeguarding (SDPS) must be a senior member of the management team who is to have relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is to be available at all times, for example, a designated deputy.
The Senior Designated Person for Safeguarding will be responsible for ensuring:
• agreed policies and procedures are to be implemented in practice.
• all updates, issues and concerns are to be communicated to all ICT users.
• the importance of online safety in relation to safeguarding is to be understood by all ICT users.
• the training, learning and development requirements of early years practitioners and their managers are to be monitored and additional training needs identified and provided for.
• an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities where deemed appropriate.
• any concerns and incidents are to be reported in a timely manner in line with agreed procedures.
• the learning and development plans of children and young people will address online safety.
• a safe ICT learning environment is to be promoted and maintained.

3.3 Early years practitioners and their managers.
Early years practitioners and their managers will ensure:
• the timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
• ICT equipment is to be checked before use and all relevant security systems judged to be operational.
• awareness will be raised of any new or potential issues, and any risks which could be encountered as a result.
• children and young people are to be supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
• online safety information is to be presented to children and young people as appropriate for their age and stage of development.
• children and young people will know how to recognise and report a concern.
• all relevant policies and procedures are to be adhered to at all times and training undertaken as is to be required.
3.4 **Children and young people**

Children and young people will be encouraged to:

- be active, independent and responsible learners, who will contribute as appropriate to policy and review.
- abide by the Acceptable Use Agreement as to be approved by peers, early years practitioners and their managers, parents and carers.
- tell a familiar adult about any access of inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent).

3.5 **Parents and carers**

3.5.1 Parents and carers are to be encouraged to sign Acceptable Use Agreements alongside their children and to share responsibility for their actions and behaviours. This will ensure a consistent message is to be communicated to all.

3.5.2 A copy of an Acceptable Use Agreement is to be provided to parents and carers on enrolment of their child at the early years setting. This will be reviewed on an annual basis thereafter. It will be an expectation that parents and carers will explain and discuss the Acceptable Use Agreement with their child to ensure that it is to be clearly understood and agreed. Children and young people will also be encouraged to sign the Acceptable Use Agreement alongside their parent or carer. Records of all signed agreements are to be kept on file.

3.5.3 Parents and carers will also be required to sign additional Acceptable Use Agreements if they are to undertake any voluntary work within the early years setting and/or participate on associated trips or visits. Further agreement is to be sought if parents and carers are to be given remote access to ICT systems, such as a learning environment, electronic portfolio or remote webcam.

4 **Acceptable use by early years practitioners and their managers.**

4.1 Early years practitioners and their managers should be enabled to use work-based online technologies:

- to access age appropriate resources for children and young people;
- for research and information purposes;
- for study support.

4.2 All early years practitioners and their managers will be subject to authorised use as agreed by the Senior Designated Person for Safeguarding (SDPS).

4.3 Authorised users will have their own individual password to access a filtered internet service provider. Users are not generally permitted to disclose their password to others, unless required to do so by law or where requested to do so by the Senior Designated Person for Safeguarding. All computers and related equipment are to be locked when unattended to prevent unauthorised access.
4.4 All early years practitioners and their managers are to be provided with a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they must sign, date and return. A signed copy is to be kept on file.

4.5 The use of personal technologies will be subject to the authorisation of the Senior Designated Person for Safeguarding, and such use will be open to scrutiny, monitoring and review.

5 In the event of misuse by early years practitioners or their managers.

5.1 Should it be alleged, that an early years practitioner or manager is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report is to be made to the Senior Designated Person for Safeguarding and the registered person immediately. Should the allegation be made against the Senior Designated Person for Safeguarding, a report is to be made to a senior manager and the registered person. Procedures are to be followed as appropriate, in line with the ICT Misuse Procedure, Safeguarding Policy and/or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

6 Acceptable use by children and young people

6.1 Acceptable Use Agreements are to be used to inform children and young people of the appropriate behaviours expected to ensure online safety. Children and young people will also be informed of the behaviours which will be deemed unacceptable. This will allow children and young people to take some degree of responsibility for their own actions.
6.2 In understanding Acceptable Use Agreements, children and young people will become aware of the potential risks associated with misuse and the sanctions which will be applied, where necessary.

6.3 The Acceptable Use Agreements are shared and agreed with children and young people and will be displayed as a reminder.

7 In the event of misuse by children and young people

7.1 Should a child or young person be found to inappropriately misuse ICT the following sanctions will be applied:

- **Step 1:** Should it be considered that a child or young person has deliberately misused ICT by not adhering to the Acceptable Use Agreement, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

- **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a senior manager and the most appropriate course of action will be agreed.

- **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children’s Social Care.

“To succeed, children need a range of opportunities to explore and use ICT resources such as cameras, dictaphones and computers. They also need to gain an understanding of why it’s important to use resources safely and appropriately to support their learning.”

Meryl Wilson, Early Years Advisor, Plymouth City Council
7.2 In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

7.3 The ‘Hectors World Safety Button’¹, is to be available to children and young people where online access is to be enabled. At a push of a button, the child’s view of the screen will be obscured. Adults will immediately be alerted and should take immediate and appropriate action. Should a child or young person be considered to be subject to potential abuse, sexual requests or other inappropriate contact, the CEOP Report Abuse button² is to be used to make a report and further advice is to be sought.

8 Acceptable use by parents and carers

8.1 Partnership working with parents and carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable and unacceptable behaviours. Parents and carers will therefore be asked to sign an Acceptable Use Agreement together with their child in order to promote this shared message.

8.2 Parents and carers are to be encouraged to contribute to the Acceptable Use Agreement and should be advised to use it should their child access similar technologies at home.

8.3 Should parents or carers wish to use personal technologies, such as cameras within the setting environment, authorisation must be obtained from the Senior Designated Person for Safeguarding. Specific guidelines for the use of such technologies must be followed.

¹ Hectors World Safety Button is a free download from Becta, to help protect children and young people when they are online (www.thinkuknow.co.uk)

² CEOP – Child Exploitation and Online Protection Centre Report Abuse button is used to make an instant report to the police in respect of online abuse (www.ceop.gov.uk).
9 Acceptable use by visitors, contractors and others

9.1 All individuals who affect or come into contact with the early years setting are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with children and young people. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.
10 Links to other policies

10.1 Behaviour Policy
10.1.1 The Behaviour Policy is to contain up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyber bullying.
10.1.2 It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the ‘real’ and ‘cyber’ world and this is to be reflected in all relevant policies.

10.2 Safeguarding Policy and ICT Misuse Policy
10.2.1 The Safeguarding Policy and the ICT Misuse Policy are to be referred to when dealing with any incidents that should occur as a result of the intentional or unintentional misuse of ICT. Any allegations of abuse or other unlawful activity are to be reported immediately to the Senior Designated Person for Safeguarding who will ensure procedures outlined in the Safeguarding Policy are followed with immediate effect.

10.3 Personal, Social and Emotional Development (PSED)
10.3.1 The promotion of online safety within PSED activities is to be considered essential for meeting the learning and development needs of children and young people. Key messages to keep children and young people safe are to be promoted and should be applied to both online and offline behaviours.

10.4 Health and Safety Policy
10.4.1 The safe use of ICT is to be included within the Health and Safety Policy, and should also include guidelines for the use of display screen equipment. The detrimental impact of prolonged ICT use on children’s brain development should also be addressed.

Authorisation and review

Agreed by: 

Authorised signatory: 

Date: 

Date of review:
Chapter 3

Internet Policy
Those adults who work with particularly vulnerable children need to be familiar with the broad spectrum of online risks facing children, and how they can support and empower children and young people to address them.

Professor Tanya Byron
Chapter 3: 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 ‘time-out’ 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 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.

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. 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’\(^2\) 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\(^3\).

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.

5.3.10 Where children and young people are to access online communications and communities, it will be considered best practice for them to adopt a nickname which will protect their identity and ensure anonymity.

\(^2\) http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00311/

\(^3\) General Teaching Council ‘Demonstrate honesty and integrity and uphold public trust and confidence in the teaching profession’.
5.4 Managing multimedia technologies (including Web2 and 3G technologies)\(^4\)

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 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 is to be restricted 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.

\(^4\) Web 2 – second generation of web communications (for example, social networking sites). 3G – next generation of mobile/wireless technologies.
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 It 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. Cyber-bulling, 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

Agreed by:

Authorised signatory:

Date:

Date of review:
“Technology isn’t toxic, but the world is – and if we don’t engage with our children, if we don’t understand the benefits technology brings them and the risks that come attached, then we’re not doing our job. Staying up to date and involved isn’t easy, but then, what part of [childcare] is?”

TechRadar UK 2009
Chapter 4: Camera and Image Policy

1 Introduction

1.1 The use of cameras should be considered an essential and integral part of everyday life. As such, children and young people and early years practitioners and their managers are to be encouraged to use such technology in a positive and responsible way.

1.2 It has to be recognised however, that digital technology has increased the potential for cameras and images¹ to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed.

1.3 Practical steps must be taken to ensure that the use of cameras and images will be managed sensitively and respectfully. A proactive and protective ethos is to be reflected which will aim to promote effective safeguarding practice.

1.4 It must however be acknowledged that technology itself will not present the greatest risks, but the behaviours of individuals using such equipment will.

2 Aim

2.1 The Camera and Image Policy will aim to ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is to be in line with legislative requirements and will aim to respect the rights of all individuals.

3 Scope

3.1 The Camera and Image Policy will apply to all individuals who are to have access to and/or be users of work-related photographic equipment. 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 Camera and Image Policy will apply to the use of any photographic equipment. This will include mobile phones and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

4 Responsibilities

4.1 The Senior Designated Person for Safeguarding (SDPS) is to be responsible for ensuring the acceptable, safe use and storage of all camera technology and images. This will include the management, implementation, monitoring and review of the Camera and Image Policy.

¹Photographic, digital, video and audio recordings.
Chapter 4: Camera and Image Policy

4.2 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 Legislative framework


5.2 All images will be used in a manner respectful of the eight Data Protection Principles.

5.3 This means that images will be:
   • fairly and lawfully processed
   • processed for limited, specifically stated purposes only
   • used in a way that is adequate, relevant and not excessive
   • accurate and up to date
   • kept on file for no longer than is necessary
   • processed in line with an individual’s legal rights
   • kept securely
   • adequately protected if transferred to other countries.

Wherever practical, cameras and other photographic equipment will be designated for work-related purposes only. Such equipment must be booked and signed out accordingly. The use of personal photographic equipment is to be avoided. Should it be considered that such use is not to be precluded for a given reason, explicit authorisation must be obtained from the Senior Designated Person for Safeguarding and all relevant details of use are to be recorded.

6 Code of conduct

6.1 All early years practitioners and their managers must ensure that the policy and procedures included herein are to be adhered to at all times. The Camera and Image Policy must be considered in conjunction with the Acceptable Use Policy and the ICT Misuse Policy.

6.2 The use of cameras and other photographic equipment is only to be authorised by the Senior Designated Person for Safeguarding. Early years practitioners and their managers should only use such equipment for purposes as designated by the Senior Designated Person for Safeguarding. It must be recognised that individuals may be given different levels of responsibility in terms of authorised use.

6.3 Early years practitioners and their managers must report to the Senior Designated Person for Safeguarding to book out cameras or other photographic equipment. The Senior Designated Person for Safeguarding will be responsible for ensuring that the following information is to be recorded each time equipment is booked out:
   • Name of individual using the equipment.
   • Date and time equipment is booked in and out.


Chapter 4: Camera and Image Policy

- Type of equipment used.
- Purpose.
- Any difficulties encountered or concerns reported.

6.5 The use of personal USB sticks, the transferring of images via free unfiltered web mail or via mobile media is be avoided. Should remote access be given to servers or systems where images are to be stored, access will only be given as authorised by the Senior Designated Person for Safeguarding.

6.6 The Senior Designated Person for Safeguarding must reserve the right to view any images taken and/or to withdraw or modify an individual’s authorisation to take or make images at any time. Early years practitioners and their managers must ensure that all images are available for scrutiny and be able to justify any images in their possession.

6.7 The Senior Designated Person for Safeguarding will be responsible for ensuring the safe storage of all images, in accordance with the Camera and Image Policy.

6.8 Early years practitioners and their managers are to have a duty to report any concerns relating to potential misuse. Clear whistle-blowing procedures are to be in place. An anonymous reporting system will also be promoted and used to facilitate this process.

7 Consent

7.1 Statement of intent

7.1.1 General signed consent to take photographs or record images of children will be requested from the parent or carer on enrolment of their child. The purpose for taking any images is to be clearly explained and agreed. Any consent given is to be reviewed on a regular basis (of a period of no more than one year) until such time the child or young person will no longer attend the setting. This consent will cover the taking of images for general purposes, such as taking photographs which will be used to document children’s learning.

7.1.2 Consent must be requested because an image of a child or young person is considered to be personal data under the Data Protection Act 1998 and consent must be obtained as a requirement of the Act. The requirement for consent will be applied to all children and young people under the age of 18 years (or from the young person, if deemed to be competent to make such a judgement, from the age of 12 years). The child’s view is however to be considered at all times, regardless of age.

7.1.3 It should be recognised that some children and young people will be more vulnerable than others, for example disabled children, children in care, those with a child protection or child in need plan, children with English as an additional language, black, minority and ethnic children and those who have been subject to domestic abuse. For a range of reasons, such children’s security may be compromised more than others, and therefore extra precautions must be considered in such circumstances.
7.2 Procedures

7.2.1 Prior consent will always be obtained in writing before any images will be taken. Verbal consent will not be accepted under any circumstance. If it should not be possible to obtain prior written consent, no images will be taken involving the individual child or young person concerned.

7.2.2 Individuals who do not have parental responsibility, such as childminders, friends or other relatives will not be able to give such consent. Only consent provided by a parent or carer with parental responsibility is to be accepted.

7.2.3 The parent or carer will reserve the right to refuse or withdraw their consent at any time. Partial or restricted consent may also be given where deemed necessary by the parent or carer.

7.2.4 Specific consent for the use of images for purposes other than those previously stated and agreed will be requested, for example, should images be required for publicity materials or to support the training needs of early years practitioners and their managers. Such consent will detail how the photographs are to be used and for what period of time such permissions will cover.

7.2.5 Images must not be used for anything other than the stated purposes; unless additional revised consent is to be obtained. A copy of the relevant image will be stored with the specific consent form.

7.2.6 Images of children who are to no longer attend the early years setting will not be used, unless specific consent has been obtained to cover this extended period. Generally consent to use images will lapse should a child leave the early years setting.

7.2.7 Images of children if held for which consent has never been given are not to be used, unless the specific consent of the parent or carer is to be obtained. Should it not be possible to obtain such consent, such images are to be returned to the individual concerned or destroyed.

“This idea that the way forward lies in finding an exact middle path between opposites is of extraordinary importance ....”
Christopher Brooker
Chapter 4: Camera and Image Policy

8 Images

8.1 Statement of intent

8.1.1 It must be recognised that children and young people could be exposed to potential risk should images be misused, including:

- the making, taking and distribution of inappropriate and indecent images.
- grooming (the process by which child sex offenders and paedophiles will befriend victims through direct or indirect contact, often preceded by efforts to gain personal information about the child or young person).

8.1.2 It must be remembered that such incidents fortunately remain very rare; but it should also be understood that detailing such concerns will often raise further anxieties and will make many individuals feel uncomfortable. It must be acknowledged however, that the first step towards minimising any danger will be to have a fuller understanding of what constitutes a risk and what behaviours may compound it.

8.1.3 Protective and precautionary measures should therefore be considered when taking, making or using images of children. It is to be ensured that all early years practitioners and their managers are aware of the potential for images to be subject to misuse; and therefore will be expected to agree and sign up to an Acceptable Use Agreement (in line with the Acceptable Use Policy).

8.2 Procedures

8.2.1 The purpose and context for any proposed image should always be considered.

It must be determined whether taking a photograph or video, for example, will be the most effective option or whether alternative methods of capturing information are to be judged more appropriate in the given circumstance.

8.2.2 Careful consideration must be given before involving young or vulnerable children who may be unable to question why or how activities are to take place.

8.2.3 Sensitivity must be shown to any child or young person who is to appear uncomfortable; and the potential for misinterpretation is to be recognised. Images will therefore not be taken of any child or young person against their wishes. Coercion must not be used to encourage a child or young person to participate when it has been indicated that they clearly do not want to be involved. A child or young person's right not to be photographed is to be respected.

8.2.4 The taking or making of images of a child or young person in a one to one situation with an adult is to be avoided whenever possible; unless there is an agreed, specified reason for doing so. It must be recognised that the context of such situations are likely to be perceived as sensitive and the use of cameras will be seen as intrusive and open to misinterpretation. It is to be recognised that this may leave both the adult and child in a vulnerable position and is therefore not to be considered accepted practice.
8.2.5 It is to be recognised that individual close up pictures of a child or young person often provides little context or purpose, and most often, an image of a group of children will show an activity or situation to better effect. Unnecessary close up pictures of an individual child or young person with no surrounding context or purpose are therefore to be avoided. The vast majority of photographs taken in the setting environment will therefore be general shots of whole or small group activities.

8.2.6 Where group photographs of children and young people are to be planned, permission must be obtained from all parents and carers. If any parent or carer has indicated that their child is not to have a photograph taken then a group photograph will not be considered appropriate.

8.2.7 Photographs are not to be taken of any child or young person should they suffer an injury; whether it is to be considered accidental or non-accidental. This will be deemed a misuse of power which will potentially cause the child or young person to become distressed or to feel humiliated. Where necessary, medical help will be sought, and in the case of a suspected non-accidental injury the Safeguarding Policy will be implemented with immediate effect.

8.2.8 All images to be taken should represent the diversity of the children and young people who attend the early years setting. No child is to be favoured in photographs.

8.2.9 Images which could be considered to cause distress, upset or embarrassment must not be used.

8.2.10 Images of children and young people must only be taken when they are in full and suitable dress. In no circumstances, are images to be taken of children or young people in any state of undress. Should children and young people be participating in sport activities, careful consideration must be given to the appropriateness of taking such images, in particular the angle of which shots may be taken.

8.2.11 The taking or making of images in sensitive areas of the early years setting, for example, toilet cubicles and changing areas are not to be permitted.

8.2.12 It should be ensured that a child or young person’s name or any other identifying information does not appear in any caption or accompanying text alongside their photograph, for example, on displays, documentation panels and name cards. Particular care is to be taken where such images are likely to be viewed by others, including the general public.

8.2.13 It is to be ensured that if, on occasion, a child or young person is to be named (for an agreed reason) in any published text, for example, in the prospectus, a photograph of the child will not appear.

8.2.14 The minimum amount of information possible is to be provided to preserve the identity of children and young people at all times. No personal details, such as home telephone numbers,
email or home addresses are to be disclosed in any written or verbal communications. This is to include information that will contribute to the personal profile of a child or young person.

8.2.15 Consideration will always to be given to where images are to be published. This will also include where parents are encouraged to be involved with learning platforms, such as ‘My First Place’ and ‘Merlin’. These systems must be designed to enable parents and carers to access their own child’s photographs and work safely.

8.2.16 It must be understood that the need to obtain consent for the use of images, is to be applied to adults as well as children.

9 Using images of children supplied by a third party

9.1 Statement of intent

9.1.1 It must be recognised that photographs and other images are subject to copyright, which will generally rest with the photographer. Prior permission must therefore be obtained before such images are to be used.

9.2 Procedures

9.2.1 Before using any image supplied by a third party, it is to be ensured that the third party owns the copyright and that consent has been given in writing by the individual(s) concerned to use the image.

9.2.2 Where a third party provides such photographs/images, they will be obliged to confirm in writing that they have the express consent of the parent or carer to use the said image, where applicable.

10 Use of images of children by the media

10.1 Statement of intent

10.1.1 There may be occasions where the press are invited to a planned event to take photographs of the children and young people who are to take part. It should be noted that the press enjoy special rights under the Data Protection Act, which permit them to publish material for journalistic purposes.

10.1.2 Generally, parents and carers will take pride in ‘press cuttings’. For the majority, this pride will often outweigh any fears about the image and/or information being subject to misuse. However, some parents may object to information about, and images of, their own children being published. As a result, it is to be ensured that parental/carer consent will be sought before the press is to be given any access to children and young people. Should a parent or carer choose not to give permission for their child to be photographed in such circumstances, this right must be observed at all times.
10.2 Procedures

10.2.1 The manner in which the press will use images is to be controlled through relevant industry codes of practice as well as the law. In this way a check is to be put on the potential improper use of images of children and young people by the press. Additional checks will however also be carried out by the Senior Designated Person for Safeguarding. This will ensure that broadcasters and press photographers are to be made aware of the sensitivity which must be considered in respect of detailed captioning, one to one interviews, and close up sports photography.

10.2.2 Where a press photographer is to be invited to celebrate an event, every effort will be made in advance to ensure that the newspaper’s (or other relevant media) requirements are able to be met. Where, for example, a newspaper is to be invited to take photographs of children and young people, it is unacceptable for their names to be completely withheld. Newspapers will be very unlikely to print anonymous photographs. An agreement will therefore be sought between parents and carers and the press which will request that first names only will be published. Responsibility and liability however cannot be held for the actions of a third party organisation, should they choose not to abide by any such agreement once in place.

10.2.3 Consideration will therefore be given to the requirements of the press before any planned event. Parental/carer permission/opinion will be the key factor in making a decision as to whether the press will be invited or not. This may mean that only those children, whose parents or carers will be happy for photographs and names to be published, can be given the opportunity to be involved in such events.

10.2.4 Should it not be considered possible or appropriate to limit the children and young people who are to be photographed, for example, because a specific group of individuals are to have achieved something special (and parental permission regarding the publication of first names is to be withheld by one or more of the group) efforts will be made to negotiate a revised agreement with the press which must be deemed acceptable to all parties. Should it not be possible for such an agreement to be reached, the option of newspaper publicity will have to be forgone.
10.2.5 The identity of any press representative will be verified. Access will only be permitted where the event is to be planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances. In the event that the press should turn up uninvited, for reasons beyond the control of the setting, every reasonable effort will be made to ensure that children and young people and parents and carers are protected from any press intrusion.

10.2.6 Every effort will be made to ensure the press abide by any specific guidelines should they be requested by the setting. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the setting is to be considered to have acted in good faith.

11 Use of a professional photographer

11.1 Statement of intent
11.1.1 It will be ensured that any professional photographer who is to be engaged to record any events will be prepared to work according to the terms of this policy document and the following guidelines:
   • In the context of data protection legislation, the photographer will be considered a ‘data processor’ and any agreement with them will be in accordance with the Data Protection Act 1998.
   • Photographers will only be used where they will guarantee to act appropriately to prevent unauthorised or unlawful processing of images; and will insure against accidental loss or destruction of, or damage to, personal data.

11.2 Procedures
11.2.1 Photographers will be asked to sign an agreement which will aim to ensure:
   • compliance with the Data Protection Act 1998.
   • images are only to be used for a specified purpose and will not be used in any other context.
   • images will not be disclosed to any third party unless it is to be a specific requirement to do so in order to fulfil the requirements of the agreement. Such use will also be subject to parental/carer permission.

11.2.2 Only reputable photography agencies and/or professional photographers will be used. Evidence of such authenticity will be required.

11.2.3 Details of any checks regarding suitability, which are to include evidence of Criminal Record Bureau checks, will be requested. Photographic identity will be checked on arrival. Should there be any concerns in respect of the authenticity of any photographer, entry will be refused. Such concerns will be reported as is to be deemed appropriate.

11.2.4 Photographers are to be treated as any other visitor. As such, appropriate levels of supervision will be in place at all times. This will ensure that no unsupervised access to children and young people will be given.
12 Children photographing each other

12.1 Statement of intent
12.1.1 Children may on occasion be given the opportunity to photograph each other and their surroundings. This practice will often occur during off-site activities and for most children it will be normal practice to take photographs to record a trip or event. Children may also be given access to cameras within the setting environment to support their learning and development needs. These activities will be encouraged in a safe and enabling environment.

12.2 Procedures
12.2.1 Early years practitioners and their managers will be required to discuss and agree some age appropriate acceptable use rules with children and young people regarding the appropriate use of cameras.

12.2.2 Nevertheless there may be occasions where children will take inappropriate images, including photographs which may show friends and other children in a state of undress. This practice will be discouraged, and parents will also be advised to monitor their child’s use of cameras within the home and social environment.

13 The right of parents and carers to take photographs and videos

13.1 Statement of intent
13.1.1 Parents and carers will not be covered by the Data Protection Act 1998 if they are to take photographs or make a video recording for their own private use. The Act will therefore not prevent parents and carers from taking photographs or making video recordings of their own children within the setting environment, for example, during nativity plays.

13.1.2 The right to refuse parents and carers the opportunity to take photographs and make videos is however to be reserved on health and safety grounds. This right will be implemented should it be deemed appropriate. For example, if an excessive use of flashlights and/or bulky and noisy equipment are to be considered a potential health and safety risk.

13.2 Procedures
13.2.1 Parents and carers will be required to complete a Photography Request Form should they wish to take or make any recordings within the setting environment. Authorised use will only be permitted on agreed dates and times, and within designated areas of the setting.
13.2.2 Before a photography request can be authorised, consent will need to be obtained from all parents and carers of other children who may be captured in any photograph or video. Should it not be possible, to gain consent from the parents and carers of all children who may be implicated, there will be no option but to refuse an open request to take or make images. Consideration will however be given to organising a one-off photograph opportunity which will only involve those children for who consent has been obtained.

13.2.3 Parents and carers will only be permitted to make recordings or take photographs of any event for their own personal use. The use of such images and recordings for any other purpose, without express permission, will be a breach of the Data Protection Act 1998.

13.2.4 Parents and carers who are to be authorised to use photographic equipment must be encouraged to be mindful of others when making and taking such images. This will be to ensure minimum disruption to other parents and carers during any event or production. Care must be taken to ensure the view of others will not be obscured and intrusive photography or filming must be avoided at all times. The right to withdraw consent will be maintained and any images or filming must be open to scrutiny at any time.

13.2.5 Every effort must be made to ensure that individuals with no connection to the early years setting are to be given no opportunity to film covertly. Early years practitioners and their managers are to have the authority to question anybody they do not recognise (subject to their own safety being ensured) should they be observed using any photographic equipment at events and productions or within the general vicinity. Care will be taken at all times to prevent any opportunist photography or filming taking place.

“Mummy, at school, we aren’t allowed to push in front of each other when we line up”.

“That’s good, because it is not polite to push in”.

“So why is it that motorbikes are allowed to push in when we are driving?”

“Bikes can be rude like that sometimes”.

“But mummy, it is the ‘man’ not the bike who is in the wrong…”

(Child, aged 6 years).
14 Closed-circuit television (CCTV)

14.1 Statement of intent
14.1.1 CCTV is to be used for the following purposes:
• To control access.
• To monitor security.
• For site management, for example monitoring incorrect parking, manoeuvring vehicles and delivery arrivals.
• For monitoring purposes, particularly within the building, in corridors and areas out of sight or not frequently trafficked by early years practitioners, for example in the vicinity of toilets (but not in toilet cubicles).
• For general and focused observations of children and young people and early years practitioners and their managers.
• To act as an effective deterrent to prevent crime and to discourage trespass.

14.2 Procedures
14.2.1 All areas which are to be covered by CCTV must be well signposted, and notifications are to be displayed so that individuals will be advised before entering such vicinity.
14.2.2 Should CCTV be used within the early years setting, it must be ensured that the manufacturer’s instructions and data protection and information sharing guidelines are to be followed at all times. This is to include the appropriate storage and disposal of all recordings.
14.2.3 Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will generally be a maximum of no more than 30 days. All recordings are to be erased before disposal.
14.2.4 Regular auditing of any stored images will be undertaken by the Senior Designated Person for Safeguarding.
14.2.5 Every effort will be made to avoid inadvertently taking inappropriate images and therefore cameras will be placed and positioned sensitively. No cameras will be pointed directly at toilet cubicles or any other sensitive areas within the setting environment.
14.2.6 During operational and out of hours periods, cameras may record inappropriate activities taking place on the premises. If such images are of a criminal nature or give any cause for concern, the information will be referred to the appropriate agency.
14.2.7 Images taken outside of operational hours will be erased in accordance with the procedures previously identified.

15 Web-cams

15.1 Statement of intent
15.1.1 Parental consent must be obtained before web-cams will be used within the setting environment. Before seeking such consent, full details of why a web-cam is to be used will be provided. This will also include information on the use of images, who is to be given authority to view them, and the security measures which will be implemented to prevent unauthorised access.

15.2 Procedures
15.2.1 The regulations which apply to web-cams regarding signage will be the same as for CCTV.
15.2.2 Consultation is to be carried out with children, young people, parents and carers, practitioners and their managers to determine if they are to be in agreement to being filmed. Written consent is to be obtained from all parents and carers.

15.2.3 The details for the storage and disposal of recordings will be the same as for CCTV.

16 Mobile phones
16.1 The Mobile Phone Policy is to be referred to.

17 Use of internet/intranet sites
17.1 The Internet Policy is to be referred to.

18 Website
18.1 Statement of intent
18.1.1 It is to be understood that the posting of images on websites may raise particular issues and concerns.

18.1.2 It must be recognised that there will be a risk that such images could be subject to manipulation and circulation without consent or even knowledge. The risk that children and young people could be exploited in some way after having their image displayed must also be acknowledged.

18.1.3 However, the value offered by websites also needs to be appreciated. They are to give children and young people extensive creative opportunities for design and development. For some children and young people this will provide a medium which will best suit their individual learning style. This will give them the opportunity to succeed and excel. Access to moderated websites is therefore to be encouraged in a safe and age-appropriate environment.

18.2 Procedures
18.2.1 Displaying images of children and young people on the setting’s external website is to be avoided, wherever possible. Should consideration be given to using images for display, explicit consent from the parent or carer will be required. Any images used will be copy-protected, include a watermark, and/or will be published in low definition to reduce the potential for misuse. Under no circumstances will a child’s photo be published on any insecure social networking sites, such as Facebook or Bebo.

18.2.2 The use of secure learning platforms such as ‘Merlin’ is however to be promoted. Photographs of children and young people can be securely posted and such use is to be encouraged. Parent or carer consent will be requested before any images are uploaded.

“The internet provides our children with a world of entertainment, opportunity and knowledge - a world literally at their fingertips. But we must ensure that the virtual world is as safe for them as this one.”

Prime Minister Gordon Brown
March, 2009
19 Learning journeys

19.1 Statement of intent
19.1.1 Under the Early Years Foundation Stage, early years practitioners and their managers are to be encouraged ‘to track children’s progress, [and have] … a system for channelling the wealth of information gathered about individual children into a manageable summary. Detailed individual observations of self-initiated activity in a particular context, photos and special moments contained in a child’s portfolio all document the child’s unique learning journey’. (Progress Matters, National Strategies). Such portfolios will often be known as learning journeys and these are to be used to document and monitor the individual learning and development progress of each child in the early years age group (birth to five years).

19.2 Procedures
19.2.1 The information contained within each learning journey is to relate to an individual, identifiable child; therefore it is to be treated as personal data. This means that such information is to be stored securely when not in use. The aim will be to avoid unauthorised access to potentially sensitive data.

19.2.2 A code of practice trust statement is to be advocated to protect and promote the welfare and individual rights of children and young people. Details of this code of practice will therefore be included on a Learning Journey Consent form. It will also be displayed on the front cover of all individual learning journeys.

19.2.3 Consent must be obtained from parents and carers should their child be photographed amongst a group of children; and where consideration is to be given to including that image in a learning journey belonging to another child. It will be anticipated that this will be a regular occurrence, as group activity shots are to be encouraged.

19.2.4 Where possible, therefore, ‘blanket’ consent will be requested from parents and carers for group images to be included in the learning journeys of other children. Parents and carers must be given the option to view any images before they are to be included in any learning journey, should they request to do so. Parents and carers will also be permitted to restrict their consent. This may mean that group images can only be included in specified learning journeys, for example, those which are to belong to close friends. Should it not be possible to obtain consent, the relevant image must not be shared across learning journeys of other children.

19.2.5 Individual learning journeys, although to be constructed by early years practitioners and their managers, are to be provided for the benefits of the individual child and their parents or carers. Parents and carers are therefore to be given the responsibility for choosing what to do with any personal data contained in the learning journey, once it is to be in their possession. However parents must be made aware that they are not permitted to ‘publicise’ another child or young person
without the express agreement of the parent or carer concerned. Parents and carers must therefore be reminded that they must not share, distribute or display said images without relevant authorisation and consent from the parents and carers of all children and young people captured in any of the photographs.

20 Early years practitioners training portfolios

20.1 Statement of intent
20.1.1 During training, early years practitioners may be required to compile portfolios which will be used to document and evidence their own learning. Part of this documentation is likely to include images of the early years practitioner working alongside children and young people participating in various activities. Should such evidence be required, parent or carer consent will be requested.

20.1.2 The Senior Designated Person for Safeguarding is to have a duty of care to ensure early years practitioners are to act responsibly in compiling the images to be included in training portfolios. Early years practitioners will therefore be monitored in their taking, making and use of such images. All images will be subject to scrutiny and regular audits will be carried out to ensure all relevant policies and procedures are to be adhered to.

20.2 Procedures
20.2.1 The Senior Designated Person for Safeguarding will oversee the compilation of images which are to be used by early years practitioners when completing training portfolios.

Any images which are to be deemed unsuitable for any reason will not be included.

20.2.2 Should images be considered inappropriate, the Senior Designated Person for Safeguarding will ensure the ICT Misuse Policy is to be applied.

21 Displaying images

21.1 Statement of intent
21.1.1 It must be ensured that still images (including those which are to be displayed in digital photo frames) and video clips are to depict children and young people in an appropriate way. The identity of individual children should also be protected. Particular caution should be taken where images are to be displayed in a public place. (The definition of a public place is to include any areas where parents and carers, members of the public and visitors are to be given access).

21.2 Procedures
21.2.1 Digital photo frames are to be used to display slideshows of children and young people at play. Specific consent must be obtained from parents and carers to allow images to be used in such a way.

21.2.2 Increased sensitivity and security procedures are to be observed when digital photo frames are to be used. The careful positioning of such frames should be considered, as they are often to be displayed in the most public areas of the setting, such as the reception.
21.2.3 Documentation panels are to be encouraged and will include, for example, photographs, observation notes and transcripts of children's communications. Information included may be personal to an individual child and should not be considered for public information. Care should therefore be taken to ensure individual children and young people will not be identifiable. Children and young people should not be named if their photograph is to be displayed; and transcripts of communications (which may add to a child’s personal profile) are to be placed randomly across the documentation panel. Transcripts are not to be attributed to individual children and young people. Should observation notes relating to individual children be displayed, confidentially must be observed at all times. Where necessary, this is to involve the removal of personal information. Alternatively a cover sheet will be placed over the top of the observation.

21.2.4 Where photographs are to be displayed in any context, the use of close up images of children and young people (particularly where they are to have been photographed against a blank background) should be avoided. Photographs of children and young people must be purposeful and show them in an appropriate context.

22 Storage and disposal

22.1 Statement of intent

22.1.1 Images are to be stored and disposed of securely. The aim will be to prevent unauthorised access, ensure confidentiality and protect identity. All images are to be stored and disposed of in line with the Data Protection Act 1998.

22.2 Procedure

22.2.1 Images will not be kept for longer than is to be considered necessary. The Senior Designated Person for Safeguarding is to ensure all photographs are to be permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

22.2.2 Should images need to be kept for a short period of time, they must be protectively stored and password protected on the computer hard drive or other appropriate storage device. Such equipment will be stored securely and access will be restricted.

22.2.3 Photographs will only be stored on portable storage devices for a temporary period. Express permission must be obtained from the Senior Designated Person for Safeguarding and effective security measures must be in place.

22.2.4 Security measures are to be the same that apply to any personal data and means that such data:

• Must be classified as protected, restricted or confidential.
• Must be marked for relevant disposal.
• Will not be removed from the site physically or electronically without suitable encryption (password protected is not enough by law).
Suitable encryption software is to be found at:
http://www.truecrypt.org/ downloads
http://www.axantum.com/ AxCrypt/Downloads.html

22.2.5 All images, including those held within learning journeys will remain on site at all times, unless prior explicit consent has been given by both the Senior Designated Person for Safeguarding and the parent or carer of any child or young person captured in any photograph. Should permission be given to take images off site, all relevant details are to be recorded, for example who, what, when and why.

22.2.6 Photographs must be disposed of should they no longer be required. It must be ensured that they will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies are not to be taken of any images without relevant authority and consent from the Senior Designated Person for Safeguarding and the parent or carer.

22.2.7 A record of all consent details are to be kept on file. Should permission be withdrawn at any time, all relevant images will be removed and disposed of. The record will be updated accordingly.

23 Security

23.1 Statement of intent

23.1.1 All images are to be handled as personal data and deemed to be of a sensitive and confidential nature. It is to be recognised that damage or distress could be caused if security is to be breached. The responsibility of being in a position of trust in handling such data must therefore be taken seriously.

23.1.2 The Senior Designated Person for Safeguarding is to be responsible for ensuring all information is handled appropriately and securely. Should there be any concerns over breaches of security, the Senior Designated Person for Safeguarding and/or the registered person will be required to undertake an investigation as is to be deemed appropriate. All such incidents are to be recorded and where necessary reported to the relevant authorities. Any actions which are to be identified as a result of any investigations must be implemented with immediate effect.

23.2 Procedures

23.2.1 Security procedures are to be monitored and reviewed at the end of every two month period.

23.2.2 Under the Data Protection Act 1998, reasonable steps must be taken to ensure the reliability and suitability of any individual who is to have access to personal data. Early years practitioners and their managers are therefore considered to be in a responsible position of trust.

23.2.3 To this effect, effective safer recruitment procedures are to be applied. Rigorous and regular checks are also to be undertaken to ensure the on-going suitability of all new and existing early years practitioners and their managers. All relevant checks must be completed before any new employee, volunteer or student is to be given access to children and/or their personal data.
23.2.4 All early years practitioners are to be required to follow confidentiality and information sharing procedures, which must be agreed to at the time of induction.

23.2.5 The following aspects of security are to be managed accordingly:

- Physical security - effective measures are to be put in place to ensure physical security and to protect against theft, including that of laptops, computers, cameras, and any personal data, including photographic images.

- Computer security – stringent measures are to be implemented to ensure computer security. Awareness will be raised in respect of technological advancements which could put online systems at risk. Security will be updated as and when it is to be required.

23.2.6 Security procedures are to be proportionate to the potential risks involved and must be subject to constant monitoring and review.

24 Authorisation and review

“The Council [UKCCIS] is a partnership where responsible organisations involved with the internet and children’s welfare come together to help children and young people enjoy the benefits of the internet whilst staying safe from the risks. As in the offline world, we can never keep children completely safe, and this is not about imposing unnecessary restrictions that undermine the internet’s benefits. But, by working together, learning from one another’s experience and reinforcing one another’s messages we can achieve more than the toughest legislation, the biggest company or the most caring charity ever could alone.”

UKCCIS, Child Internet Safety Strategy.
Chapter 5

Mobile Phone Policy
“For those agencies whose job it is to protect children and vulnerable people, the harsh reality is that if a sufficiently devious person is determined to seek out opportunities to work their evil, no one can guarantee that they will be stopped. Our task is to make it as difficult as possible for them to succeed...”

Bichard Inquiry Report, 2004, p 12 paragraph 79
Chapter 5:
Mobile Phone Policy

1 Introduction

1.1 Mobile phone technology has become more sophisticated over recent years and will continue to evolve. Wireless connections in particular are to extend the capabilities of mobile phones further; which will allow access to new content and services, such as the internet, social networking sites and instant messaging. Many mobile phones offer camera, video and audio recording as standard.

1.2 Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are to be associated risks. Children and young people must be encouraged to understand such risks to enable them to develop the appropriate strategies which will keep them safe.

1.3 As with online safety issues generally, risks to children and young people should be broadly categorised under the headings of:
   • content
   • contact
   • conduct
   • commerce.

These issues are to be managed by reducing availability, restricting access and increasing resilience.

1.4 This philosophy is to be applied to the use of mobile phones through the Mobile Phone Policy. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses as to be agreed with the Senior Designated Person for Safeguarding. Any authorised use of mobile phones is to be monitored and recorded. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

1.5 Under no circumstances are images, video or audio recordings to be made without prior explicit written consent by the Senior Designated Person for Safeguarding.
Chapter 5: Mobile Phone Policy

2 Aim

2.1 The aim of the Mobile Phone Policy is to protect children and young people from harm, by ensuring the appropriate management and use of mobile phones by all individuals who are to come into contact with the early years setting.

2.2 Children and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use.

2.3 This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

3 Scope

3.1 The Mobile Phone Policy will apply to all individuals who are to have access to and/or be users of personal and/or work-related mobile phones within the broadest context of the setting environment. 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.

4 Policy statement

4.1 It is to be recognised that it is the enhanced functions of many mobile phones that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and bullying.

4.2 It must be understood that should mobile phones be misused, there will be a negative impact on an individual’s safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

4.3 Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others.

4.4 It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

4.5 Designated ‘mobile use free’ areas are to be situated within the early years setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include:

- sleep areas
- changing areas
- toilets
- bathrooms.

5 Code of conduct

5.1 A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the children and young people in their care.
Chapter 5: Mobile Phone Policy

5.2 It is to be ensured that all practitioners and their managers will:

• be aware of the need to protect children from harm.
• have a clear understanding of what constitutes misuse.
• know how to minimise risk.
• be vigilant and alert to potential warning signs of misuse.
• avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
• understand the need for professional boundaries and clear guidance regarding acceptable use.
• be responsible for the self-moderation of their own behaviours.
• be aware of the importance of reporting concerns immediately.

5.3 It is to be recognised that studies consistently indicate that imposing rigid regulations and/or ‘bans’ on the actions of others are counterproductive and should be avoided. Such imposition will lead to a culture of suspicion, uncertainty and secrecy. An agreement of trust is therefore to be promoted regarding the carrying and use of mobile phones in the early years setting. This is to be agreed by all service users, including all children, young people and adults who are to come into contact with the early years setting.

6  Procedures

6.1 Clearly defined policies and procedures will aim to ensure effective safeguarding practices are in place to protect children from harm and exposure to behaviours associated with misuse. The need to ensure mobile phones will not cause unnecessary and/or unsafe disruptions and distractions in the workplace are also to be considered.

6.2 Acceptable use and management of mobile phones is to be agreed by all service users. There is to be a clear expectation, for example, that all personal use of mobile phones is to be limited to allocated lunch and/or tea breaks, unless it is to be otherwise agreed by the Senior Designated Person for Safeguarding. Such authorised use is to be monitored and recorded. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

6.3 The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it is to be explicitly agreed otherwise by the Senior Designated Person for Safeguarding. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Senior Designated Person for Safeguarding is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
6.4 Practitioners and their managers are to be encouraged not to use their own personal mobile phones for contacting children and young people, parents and carers. If it is to be deemed necessary, it must be with the explicit written consent of both the Senior Designated Person for Safeguarding and the parent or carer; unless it is to be considered an emergency. Care is to be taken to ensure that work mobiles are not to be exploited in a similar way.

6.5 Children and young people are to be enabled to have access to their own personal mobile phones should they choose. This will be subject to signed agreement by the parent or carer. Safe management and acceptable use of such mobile phones is to be promoted and monitored. Children and young people’s mobile phones are to be switched off or to be set on silence during the course of the day, except where express signed permission is to be given to do otherwise.

6.6 All service users, including parents, carers, visitors and contractors should be respectfully advised that their mobile phones are not to be used in designated mobile use free areas. Should it be considered necessary for mobile phone calls and/or texts to be taken or made, efforts should be made to avoid any unnecessary disturbance or disruption to children and young people. No images, video or audio recordings are to be made without prior explicit written consent by the Senior Designated Person for Safeguarding.

6.7 All individuals who are to bring personal devices into the early years setting must ensure that they hold no inappropriate or illegal content.

7 Work mobile

7.1 The use of a designated work mobile is to be promoted as it is considered to be:

- an effective communication tool, enabling text, email messages and calls to be made and received.
- an essential part of the emergency toolkit which is to be taken on short trips and outings.
- a back-up facility should landline facilities be unavailable – or where contact needs to be made outside of operational hours.

7.2 Effective security procedures are to be put in place to safeguard against any potential misuse. Only
authorised individuals are to have access to the work mobile, which is to be password protected, and to be stored securely when not in use. All use is to be recorded and monitored by the Senior Designated Person for Safeguarding.

7.3 Personal calls are not to be made on the work mobile phone, other than in circumstances to be agreed. Personal contact will be permitted to be made via the work mobile in the event of an emergency. All such communications are to be logged.

7.4 The work mobile phone is to be clearly labelled as such.

8 Driving

8.1 Practitioners and their managers who will be required to drive on behalf of the early years setting must ensure any work and/or personal mobile phones are to be switched off whilst driving.

8.2 Under no circumstances, when driving on behalf of the organisation, should practitioners and their managers make or take a phone call, text or use the enhanced functions of a mobile phone. This is also to apply to the use of hands-free and wireless connections, which are to be considered a distraction rather than a safer alternative.

9 Safe storage

9.1 A designated safe and secure area is to be made available to practitioners and their managers for the storage of personal belongings during the working day.

9.2 Practitioners and their managers should recognise that they are to leave any belongings in such storage areas at their own risk. It is recommended that should mobile phones be stored, they are to be security marked, password protected and insured. No liability for loss and/or damage is to be accepted.

10 Emergency contact

10.1 It is to be recognised that mobile phones provide direct contact to others, and will often provide necessary reassurances due to their ease of access, particularly at difficult times. Agreed acceptable use of mobile phones is to therefore be promoted. This is to afford practitioners and their managers peace of mind, by reducing stress and worry and is therefore to allow them to concentrate more fully on their work. Such use must be subject to management, monitoring and review.

“The virtual world opens up new opportunities for learning and creativity, but it also means thinking ahead of new risks.”
Becta
Chapter 5: Mobile Phone Policy

10.2 It is to be ensured that the landline telephone remains connected and operational at all times, except in circumstances beyond reasonable control. This means that the landline is to be available for emergency/urgent contact at all times.

10.3 The reliance on an answer phone is to be avoided unless the early years setting should be closed or where children are to be taken off the premises for a trip or outing. It must always be ensured that the answer phone is to be checked promptly on opening or return.

11 Authorisation and review

Agreed by: ____________________________

Authorised signatory: ____________________________

Date: ____________________________

Date of review: ____________________________

“A child miseducated is a child lost.”
John F Kennedy, 1963
Chapter 6
ICT Misuse Policy
If staff understand the potential misuse of ICT they are constantly alert and able to identify misuse - this is the vital ingredient. We have gone beyond the notion that screening, banning and blocking are answers - monitoring is the key, and a responsibility for all those coming into contact with children.”

Tony Staunton, Plymouth Safeguarding Children’s Board 2009
Chapter 6: ICT Misuse Policy

1 Aim

1.1 The ICT (Information and Communication Technology) Misuse Policy will aim to ensure any allegation, which is to be made in respect of the intentional or unintentional misuse of any online technologies, is to be addressed to in a responsible and calm manner. This is to include any known or suspected breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Phone Policy.

1.2 Allegations are to be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT Misuse Policy will also outline the sanctions that are to be applied should an incident occur.

1.3 The overall priority will be to ensure the safety and wellbeing of children and young people at all times. Should it be suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the Safeguarding Policy and Procedures must be implemented with immediate effect. These procedures are also to be followed should an allegation of abuse be made against any employee, manager, volunteer or student. The Safeguarding Policy is to take precedence over all others, and referrals must be made to the appropriate agency as deemed necessary.

2 Scope

2.1 The ICT Misuse 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.

2.2 The policy will be implemented in respect of any potential breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Phone Policy.
Chapter 6: ICT Misuse Policy

3 Responsibilities
3.1 The registered person and the Senior Designated Person for Safeguarding are to be responsible for ensuring that the procedures outlined herein will be followed. These procedures are to be considered should an allegation of misuse be made against a child, young person or adult.

4 Policy statement
4.1 Clear and well-publicised policies and procedures which will influence practice, are to be considered the simplest and most effective way for the safe use of ICT to be upheld. Such policies and procedure should ensure the promotion of acceptable use and clearly define those behaviours which are not. The sanctions to be imposed in respect of any incidents of misuse should be identified.

4.2 It will be ensured that:
• relevant online safety policies and procedures will be fully implemented, monitored and reviewed. These policies and procedures are to be rigorous, manageable and reflective of practice; and are to be shared with all ICT users. The Senior Designated Person for Safeguarding will be responsible for the management of such policies.
• all ICT users are to be made aware of possible signs of potential misuse. Adults, in particular, will be responsible for observing practice and behaviours, so that any significant changes in such are to be identified at the earliest opportunity.
• all ICT users are to be made aware that the misuse of ICT and/or breaches of relevant policies and procedures are to be taken seriously. All ICT users are to be made aware of the potential sanctions that could be applied should such concerns be raised.
• effective reporting and whistle-blowing procedures are to be in place and promoted.

4.3 It is to be acknowledged, however, that no system or procedure can be considered 100 per cent safe, secure and fool-proof. It should therefore be accepted that the potential for ICT to be misused, whether intentionally or unintentionally will remain. The aim of the online safety policies will therefore be to minimise such opportunities and risk.

5 Procedures
5.1 General
5.1.1 All incidents are to be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions are to be put in place.

5.1.2 The context, intention and impact of each incident are to determine the response and actions to be taken. This will allow for a degree of flexibility as to how sanctions are to be applied, subject to the need for other policies to be implemented. For example, a series of minor incidents by one individual is likely to be treated differently than should it be deemed a one-off occurrence; similarly unintentional and intentional
Chapter 6: ICT Misuse Policy

access to inappropriate websites are to instigate different levels of intervention and sanctions.

5.1.3 All online safety incidents are to be recorded and monitored, and any potential patterns in behaviours should be identified, to enable such issues to be addressed proactively and for protection to be afforded.

5.1.4 Misuse is to be categorised under the three headings of ‘minor incidents’, ‘significant incidents’ and ‘serious incidents’.

5.2 Minor incidents
5.2.1 The following procedure is to be followed should an incident be considered minor.

• The incident is to be reported to the Senior Designated Person for Safeguarding. A written incident record is to be made, and the situation is to be monitored.

• The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident is to be escalated to a ‘significant’ or ‘serious’ level.

• Sanctions are to be applied in accordance with the Acceptable Use Policy.

5.3 Significant incidents
5.3.1 There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is not to be considered suitable in a childcare environment and/or to be age appropriate.

5.3.2 An open reporting policy is to be in place which means that all inadvertent breaches and access to inappropriate materials must be reported. The non-reporting of such breaches are to result in the concern being escalated.

5.3.3 The following procedure is to be followed should an incident be considered significant.

• The incident is to be reported to the Senior Designated Person for Safeguarding. A written incident record is to be made.

• The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident is to be escalated to a ‘serious’ level.

• Appropriate action is to be agreed between the Senior Designated Person for Safeguarding and the registered person.

• If the incident should relate to the inadvertent access to an inappropriate website, it is to be added to the banned or restricted list and filters are to be applied, where relevant.

• Sanctions are to be applied in accordance with the Acceptable Use Policy.

• In respect to misuse by children and young people, parents and carers are to be informed of the alleged incident and are to be advised of any actions to be taken as a result.
5.4 Serious incidents

5.4.1 It must be ensured that all serious incidents will be dealt with promptly and reported to the Senior Designated Person for Safeguarding and the registered person immediately.

5.4.2 The context, intention and impact of the alleged misuse must be considered.

5.4.3 Appropriate action is to be agreed between the Senior Designated Person for Safeguarding and the registered person. All details are to be accurately and legibly recorded. The reason why any decision is made will be also be noted.

5.4.4 Should it be considered at any stage that a child or young person is or has been subject to abuse of any form, the Safeguarding Policy will be implemented with immediate effect. A referral will be made to Children’s Social Care and the Police, where applicable.

5.4.5 Should the incident relate to an allegation made against an employee, manager, volunteer or student; and there is a suggestion that a child or young person has been subject to any form of abuse, the Safeguarding Policy will again be implemented with immediate effect. The Local Authority Designated Officer must be contacted in the first instance in respect of any allegation made against an adult. The Police and Ofsted must also be contacted.

5.4.6 It is to be ensured that no internal investigation or interviews are to be carried out in respect of any allegations, unless it is to be explicitly requested otherwise by an investigating agency.

5.4.7 It is to be fully recognised that should allegations of abuse be made, Children’s Social Care, the Police and/or the Local Authority Designated Officer will be the investigative bodies. It must therefore be ensured that no action is to be taken which could compromise any such investigations.

5.4.8 Where applicable, any hardware implicated in any potential investigations of misuse is to be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.

5.4.9 Internal disciplinary procedures must not be undertaken until investigations by the relevant agencies are to have been completed. Legal or human resources advice should be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.

“The internet presents tremendous opportunities for young people, but with this come risks. Online safety is an issue of growing importance for parents and families who rightly have concerns about what their children see and do online.”

Ed Balls, Children’s Secretary, 2009.
5.4.10 On completion of both internal and external investigations, or sooner where it is to be deemed appropriate, an online safety review is to be undertaken and policies and procedures are to be amended and updated as necessary. A consultation on any proposed revisions will be held with all ICT users as appropriate. Revised policies and procedures will be circulated as applicable.

5.4.11 By nature, serious incidents will most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment through the use of portable media devices, such as mobile phones or grooming. In such situations, these incidents may be instigated by a child, young person or adult.

5.4.12 The following incidents must always be reported to the Police, Children’s Social Care, Local Authority Designated Officer and Ofsted:

- Discovery of indecent images of children and young people.
- Behaviour considered to be ‘grooming’.
- Sending of obscene materials.

It should be understood, that by not reporting such incidents, an offence may be committed.

5.4.13 The seriousness of such allegations is to be fully recognised, and it must be ensured that all such incidents are to be reported to the Police immediately. No attempt is to be made to download, print or send any materials found. It should be understood that further offences could be committed by doing so.

5.4.14 Should potentially illegal material be discovered, as far as is reasonably practical, the equipment or materials found will not be touched. Computers or other devices will not be switched off unless it is authorised to do so by the Police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer remain on).

6 Illegal material and activities which must be reported to the Internet Watch Foundation.

6.1 A report is to be made to the Internet Watch Foundation should potentially illegal material, including images of child abuse be discovered. If it is unclear whether the content is to be considered illegal or not, the concern will be reported as a matter of caution.

6.2 Should it be considered that materials are inappropriate but legal, such incidents will generally be dealt with through internal disciplinary procedures. Unless alleged criminal activity and/or abuse is suspected, it will not normally be considered necessary to involve the Police or other agencies.

1 IWF Internet Watch Foundation
http://www.iwf.org.uk/reporting.htm
Chapter 6: ICT Misuse Policy

7 Media attention

7.1 It must be recognised that should a serious incident occur, it will most likely attract intense media interest and speculation. On such occasions, every possible attempt is to be made to ensure that children and young people, parents and carers are protected from such influences.

7.2 An agreed media strategy will be implemented, and statements must only be released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern will be the safeguarding and welfare of the children, young people and their families. Advice will be taken from Services for Children and Young People where appropriate before any media engagement is to be undertaken.

8 Authorisation and review

Agreed by:

Authorised signatory:

Date:

Date of review:

“Throughout the Early Years Foundation Stage [and beyond], children need opportunities to explore information, communication technology (ICT) in a range of meaningful contexts to support their learning, particularly where this reflects their interests and preferred learning style.

Practitioners will support children in using ICT resources appropriately, helping them to make sense of the world around them in a range of real situations.

Practitioners also find that using photographs, tape and video recording can be helpful to document children’s learning and development, and is an accessible way of sharing observations with children and their parents.

In addition, children and parents can be actively involved themselves in the ongoing observation and assessment process by using ICT equipment to capture special moments which celebrate achievements and identify children’s fascinations.

This adds a rich layer to the wealth of information that practitioners gather about learning and development, and will help shape decisions about what needs to be provided in the future to ensure children make the progress they are capable of, within a safe e-learning environment.

Our challenge, therefore, is to MINIMISE risks whilst MAXIMISING opportunities.”

Jo Paterson, Early Years Regional Advisor, South West, The National Strategies.
Appendices
Appendix 1: References

References

The following information sources have been considered in the course of producing this report:
Byron Report
(http://www.dfes.gov.uk/byronreview)
www.plymouthscb.org.uk
www.kent.gov.uk
www.ofsted.gov.uk
www.dcsf.gov.uk
www.becta.org.uk
www.swgfl.org.uk
www.ceop.gov.uk
www.thinkyouknow.co.uk

Author
Maria Hollett, Plymouth Services for Children and Young People

Acknowledgements
With sincere thanks to Tony Staunton, Ken Corish, Viv Venn, Simon White (Plymouth Services for Children and Young People/Plymouth Safeguarding Children’s Board).

Created by
Early Years Team (All Children First)
Plymouth Services for Children and Young People

Supported by
Plymouth Safeguarding Children’s Board

Printed by
Euro RSCG Riley,
Tudor House, 16 Cathedral Road,
Cardiff CF11 9LJ.
Tel: 029 2038 9684.
Fax: 029 2037 9050.

Publication date
28th April 2010.
1.1 Grooming

What is a child sex abuser?
A child sex abuser is an individual who is sexually attracted to both children and adults and will act on such desires. The term ‘paedophile’ is used to describe an individual who is attracted to children and young people. Perpetrator is a term that can be used to describe an individual who abuses children, young people, and/or adults, and such abuse can include physical, emotional, sexual and domestic. It can be used as a collective term to describe all forms of abuser.

Why do perpetrators like to use the internet to contact children?
The internet continues to become an increasingly common medium used by perpetrators; as they are able to gain personal information about children, including photographs, whilst essentially remaining anonymous through the creation of various aliases and a complex elaborate web of lies.
Perpetrators will often lie about who they are, what sex they are and how old they may be. They will often feel safer because they may be operating from their own homes, and have false email addresses and user names. They are likely to target the sites that children may use, such as online gaming sites.

What risks do such perpetrators present?
Potential risks include perpetrators:
• swapping and distributing images of child sex abuse online through email, social networking or instant messaging sites.
• joining with other perpetrators to create a network where they can share ‘grooming’ tips, and information on how to avoid being caught.
• gathering and sharing personal information about children and young people.
• using online blogs, forums and chat rooms with the intent and purpose of befriending and grooming children; obtaining and distributing indecent images and arranging to meet children for sex.

What is online grooming?
The Sexual Offences Act 2003 defines online grooming as:
“A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes.”

What other forms of grooming are there?
Perpetrators will purposely seek out children and young people through deliberately accessing activities children enjoy, visiting places which are popular with them, and even befriending adults, such as single parents or those who work with children.
A perpetrator will target vulnerable children and young people directly. They will also target them indirectly by befriending a vulnerable adult.
A perpetrator may glean information from a number of places, such as a documentation panel in an early years setting, to help them identify children, find out where they live, where they play and/or their likes and dislikes.
The sole purpose of grooming is for an adult to engage children in sexual acts, or to seek other forms of sexual gratification from them. The grooming techniques used will often be very sophisticated, and the web of lies constructed will be extremely believable and plausible. A perpetrator has the art of deception very fine tuned, and has the skills to build up the trust of their victim.
Appendix 2: The Risks Associated with ICT - FAQs

Once that trust is established, tactics such as blackmail, mind games, guilt and other forms of emotional and psychological abuse are used to maintain the ‘relationship’ for their own sexual gratification.

Remember – perpetrators also groom adults to get to children.

1.2 Mobile phones

**How do children use mobile phones?**

The use of mobile phones by children and young people is becoming increasingly common at an earlier age. Mobile phones are no longer simply a tool for making a call, but incorporate sophisticated technology which will enable children to use them for a variety of purposes. This may include access to the internet, WiFi, email, text, social networking sites, taking, sending and receiving photos and video clips, playing games, and downloading information.

Mobile phones increase children’s feeling of independence, and will offer parents and carers reassurance by providing them with a means of keeping in touch.

**What are the risks children and young people may encounter when using mobile phones?**

As many mobile phones now have internet access, many of the risks encountered are the same as detailed under the section, headed ‘Grooming’. The use of internet via a mobile phone however presents further concerns, as there is even less likelihood of children and young people having supervised access to the internet in this mobile form, than if they were accessing the internet at home.

These concerns also apply to the taking, making, possessing and distribution of indecent and illegal images. Such images can be changed and distorted and can end up in the hands of strangers all over the world for their own sexual gratification.

Another risk associated with mobile phones relates to ‘happy slapping’ where children and young people may be either the victims or instigator of such crimes. ‘Happy slapping’ is a form of bullying where a victim is targeted and assaulted, whilst an accomplice records the offence, often on a mobile phone. The resulting images are then distributed and shared with others as a token of achievement.

Many instances of ‘happy slapping’ aim to capture the surprise and shock of the victim and it is often a ‘comical’ affect that assailants aim for – having originated from television programmes, such as ‘Jackass’. The craze for ‘happy slapping’ has however escalated far beyond a ‘joke’, resulting in serious assaults and manslaughter charges, with both the attacker and the individual recording the event being subject to similar charges.

Increasingly other mobile technologies pose similar risks to mobile phones, as games such as DSis and PSPs now have the ability to connect to the internet, and record photo and video images. Similarly static games, such as the Wii, and Playstations will have internet access, and with the ability to connect wirelessly, parents are not always aware of their children’s use of an unfiltered environment.

1.3 Cyber-bullying

Cyber-bullying is the deliberate and calculated use of ICT resources to repeatedly intimidate, harass and bully another individual. This may be through direct contact, such as abusive texts, emails, instant messages, and through chat rooms; or indirectly through accessing and circulating personal information and posting embarrassing images or lies on social networking sites. This list is far from exhaustive.

---

1 Adapted from ‘Thinkuknow’, CEOP.
Such communications may be threatening but most often the intention is intimidation and the inappropriate use of power over another individual. Both adults and children can be victims of cyber-bullying, and it can lead to serious emotional and psychological abuse and distress, which in extreme circumstances can lead to the victim's suicide. The effects of cyber-bullying should not be under-estimated. ‘You can have 60 people bullying you on the internet, but in real life there wouldn’t be 60 people beating you up’… (Direct.gov).

Cyber-bullying often happens in ‘gangs’ which grow to such an extent that some members may not even recognise that they are bullying another individual and the harmful effects this may cause.

### 1.4 Photography

With the advent of digital technology, the risk and frequency of misuse and child abuse has risen.

There are a number of ways children may be exposed to risk through the uncontrolled use and display of photographs, including, but not exhaustively:

- Identification of individual children, including their name, likes and dislikes, who their friends and family are, what early years settings they attend, what they do at the weekend, what their house looks like… the list is endless. This provides more than sufficient information for a perpetrator to target and groom a child for sexual exploitation.

- Exposure of vulnerable children, including children who:
  - have child protection or child in need plans
  - are victims and survivors of domestic abuse
  - are disabled
  - have English as an additional language
  - are from BME or traveller families

The outcome of such exposure could lead to grooming, putting a child at risk of abduction, bullying and/or violence.

- The distortion and adaptation of photographs for inappropriate use, either through the direct recording of sexual acts themselves, or through cutting and pasting images, so that new ‘photos’ can be created. This may be achieved by using images of various children to create completely different and ‘whole’ photographs (this is particularly relevant where an indecent image has been taken by an abuser, and in an attempt to avoid detection has only taken images of the torso and lower half of the body. The upper part and face of another child may then be superimposed on the photograph to increase sexual gratification). Changing images digitally in such a way is sometimes referred to as ‘morphing’. Perpetrators may use close up photographs or high pixel photographs to alter in this way.

The rationale for using photographs in context and the recommendation to avoid single shots taken on a plain background is again to make the ‘job’ of a perpetrator more difficult. If background or distance shots of children are to be used, they are less likely to be exploited. Similarly, photographs with detailed backgrounds make it more difficult for the images of the child to be successfully and realistically altered or morphed. This is why images of children against a blank background should be avoided, as they provide an ideal opportunity for the image to be distorted and used in a totally different context.

### 1.5 What other risks are there?

Other risks can include:

- Addiction
- Health risks – the impact of early and prolonged use of technology on children’s brain development, and the danger of injuries such as repetitive strain injuries, from frequent use of gaming machines
- Gambling and debt
- Desensitising children to violence and intimacy.
Appendix 3: Plymouth Interagency E-safety Pledge

Plymouth Interagency E-safety Pledge

The Plymouth Safeguarding Children Board and its partner agencies are committed to ensuring that children and young people are safeguarded while using information and communication technology (ICT).

To ensure this commitment we pledge the following:

1. The advantages and positive aspects of using ICT will be continually promoted among children and young people.
2. Our agency will have its own Acceptable Use Policy (AUP), which will be kept up to date as technology, and its use, develops and which will be promoted among the agency’s staff.
3. Our agency will have a member of staff designated as an E-safety Officer, who is fully conversant with children and young people’s safe use of ICT and responsible for ensuring that all necessary policies and procedures and safeguarding measures are in place.
4. The AUP will be promoted and made available to children and young people using ICT and their parents/carers.
5. Electronic safeguards, appropriate to the setting, will be put in place, in line with guidance from British Education Communications and Technology Agency (BECTA: www.becta.org.uk) and the UK Council for Child Internet Safety (UKCCIS) and will be updated regularly. Reports generated from these will be used to confirm adherence to AUPs.
6. Children and young people using ICT within agencies will be made aware of their online rights, and the potential risks and dangers.
7. Children and young people will be equipped with the knowledge and encouraged to take responsibility for keeping themselves safe whilst using ICT, in line with the agency’s Acceptable Use Policy.
8. Our agency will promote Peer Mentoring as a method for children and young people to keep each other safe online.
9. Relevant members of staff will be made aware of safeguarding issues for children and young people using ICT and key staff, including those who supervise the use of ICT, will be fully informed about its safe use.
10. Procedures will be in place to ensure that action will be taken when there are concerns that the ICT equipment has been used inappropriately by users, staff or members of the public.
11. Young people, parents/carers and members of the public will be made aware of how to report concerns/whom to speak to if they feel worried about, or are aware of, the inappropriate use of ICT.

12. Young people will be consulted about, and involved in, the implementation of our pledge.

Signed

Agency (name and address)
Appendix 4: Image Consent Letter

Image Consent Letter

Date:
Dear Name of the child’s parent or carer
Reference: Name of child

This letter explains why we will need to ask for your consent before we are able to take photographs of your child during their time at (Name of early years setting).

 Generally photographs are a source of pleasure and pride. We believe that the taking and use of photographs can enhance the self-esteem of children and their families and therefore is something to be welcomed and appreciated.

We may take photographs for a number of reasons whilst your child is with us, including to:
• document what they enjoy doing
• record their learning and development progress
• display in learning journeys and/or document panels
• record special events and achievements.

We will also encourage children to be active learners, and to become involved in using cameras themselves by taking photos of their surroundings, activities and of each other.

We do however recognise that with the increase use of technologies, particularly digitally and online, the potential for misuse has become greater and we understand that this can give rise to concern. We will therefore endeavour to put effective safeguards in place to protect children and young people by minimising risk. We will seek to protect children’s identity and to limit opportunities for the taking, making and distribution of inappropriate images.

We have a Camera and Image Policy in place, which you are welcome to view or take a copy of at any time.

We are mindful of the fact that for some families, there may be reasons why protecting a child’s identity is a matter of particular anxiety, and if you have special circumstances either now, or at any time in the future which would affect or change you position regarding consent, please let us know immediately, preferably in writing.

If your child is old enough to express their own view, you may want to consult with them about categories of consent, and we invite you to use this letter to explore their feelings about being photographed at our early years setting.

Please read and complete the attached forms and do not hesitate to contact me should you have any queries.

Yours sincerely,
Appendix 5: Consent Form for Taking Images

Consent Form for Taking Images

To Name of the child’s parent or carer
Re: Name of child

Occasionally, we may take photographs of children and young people to mark special occasions and to monitor their learning and development progress. Any photos taken will be for the use of our early years setting and yourselves, and we will therefore not share them with a third party without explicit authorisation or consent.

Occasionally, we may invite the media into our early years setting to take photographs or film footage for publicity purposes and to record any special events. We will notify you of such occasions, and will seek specific permission for photographs to be taken, and potentially published at such times.

Should we wish to use any images in our publicity, in our prospectus or on the website, we will again ask for specific permission. This will be obtained alongside a copy of the image, and permission to use such image will be for a defined period of time only.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child.

Please complete as appropriate.

• I consent / do not consent to photographs of my child being taken by authorised personnel representing [name of early years setting].
• I agree / do not agree with any resulting images being displayed on walls or in digital photo frames where they may be visible at times to the general public or anywhere which could be defined as a ‘public place’.
• I understand that additional consent will be obtained should images be taken or used by a third party, used in publicity materials or in the media.
• I understand that I can withdraw my consent, or request to see photos taken at any time.
• I have read and understood the conditions of use set out below.
• I have discussed this policy with my child, and s/he is happy to be photographed, although I understand that at any time should s/he refuse or become upset, no photographs will be taken.
Appendix 5: Consent Form for Taking Images

Note:
This form is valid for the duration of your child's time at our early years setting. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your consent at any time.
I have read and understood the conditions of use.

Parent/carer’s signature:

Name: Date:

☐ 😊 I am happy for my photograph to be taken.

☐ 😞 I will tell an adult if I am ever unhappy having my photo taken.

Name of child: Age:
Dear Parent/Carer

We are staging a production/special event of

______________________________
on

We are sure some parents/carers would like to take photographs/videos of the production.

As you know we have a rigorous policy in place with regards to the taking, making and use of images and you will have previously signed a general consent form stating whether or not your child could be photographed.

In circumstances, such as productions or special events, we request specific consent before photographs can be taken by a third party.

If you wish to take photos at the production there is a strong possibility that other children will also be included within the picture. We therefore need to ensure all parents/carers who have children in the production are happy for photographs to be taken, and hence need to request their permission.

We would, therefore, be very grateful if you would complete the slip at the bottom of this letter and return it to me by xx Xxxxxxx 2010.

Note:
Should any parent/carer not agree with their child being photographed, we will consider alternative options including:
• restricting who is involved in the production/special event
• staging specific photograph opportunities

Photographs of setting productions are ones which parent/carers tend to treasure. We will therefore only prohibit the use of cameras and videos as a last resort. We hope you will support us in this.

Yours sincerely

Child’s name:  Date:

I am / am not * happy for photographs to be taken of the production/special event in which my child is due to appear on xx Xxxxxxx 2010.

(*Please delete as appropriate)

Signed:  (Parent/Carer)  Date:
Dear Parent

As part of the framework and programme of activities to support children’s learning and development, your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. These resources include access to: [adapt for individual early years setting]

- Computers • Internet • Email
- Games consoles • Digital cameras and copying and printing facilities
- Recorders and dictaphones.

We recognise the important contribution and value that such resources play in promoting children’s learning and development; however, we also recognise there are potential risks involved. We therefore have rigorous online safety policies and procedures in place.

In order to support us further in developing your child’s knowledge and understanding about online safety, please read the following rules with your child. We then ask that you and your child ‘sign’ and return the attached slip.

We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful partnership.

Full details of the Acceptable Use Policy and Internet Policy are available on request.

Hopefully, you will also find these rules provide you with an opportunity for further conversations between you and your child about safe and appropriate use of the online and digital technologies, both within and beyond the early years setting environment, such at a friend’s house or at home.

Should you wish to discuss the matter further, please do not hesitate to contact me.

Yours sincerely,
## Appendix 7: Online Safety Acceptable Use Agreement

### Child Agreement:

**Online safety acceptable use agreement return form**

<table>
<thead>
<tr>
<th>Name:</th>
</tr>
</thead>
</table>
| • I understand the agreement for using the internet, email and online tools, safely and responsibly.  
• I know the adults looking after me will help me to stay safe and check that I am using the computer to help me with my work. |
| Child Signature: |
| Date: |

### Parent/Carer Agreement:

**Online safety acceptable use agreement return form**

<table>
<thead>
<tr>
<th>Parent/Carer Signature:</th>
</tr>
</thead>
</table>
| • I have read and discussed the agreement with my child and confirm that he/she has understood what the rules mean.  
• I understand that the setting will use appropriate filtering and ensure appropriate supervision when using online and digital technologies.  
• I understand that occasionally, inappropriate materials may be accessed and accept that the setting will endeavour to deal with any incident that may arise, according to policy.  
• I understand that whilst my child is using the internet and other online tools outside of the early years setting, that it is my responsibility to ensure safe and responsible use with the support of the setting. |
| Date: |
Online Incident Log Sheet

To be completed as thoroughly as possible by practitioner or manager identifying incident

<table>
<thead>
<tr>
<th>Date(s) / times of incident:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration of incident: (e.g. One off, a week, 6 months etc.)</td>
</tr>
<tr>
<td>Description of the online safety incident: include detail of specific services or websites used (e.g. chat room, instant messenger); email addresses; usernames etc.</td>
</tr>
<tr>
<td>Why do you have concerns about this incident?</td>
</tr>
<tr>
<td>Has the information been recorded and secured? □ Yes □ No</td>
</tr>
<tr>
<td>Has any computer or hardware been secured? □ Yes □ No</td>
</tr>
<tr>
<td>If yes, who, where, when and what?</td>
</tr>
<tr>
<td>Who was involved and how do you know this? Is there any evidence to suggest that false names/details have been given? <strong>Give full details of real names and email addresses etc where known.</strong></td>
</tr>
</tbody>
</table>
Appendix 8: Online Incident Log Sheet

How was the incident identified? E.g. by member of staff, informed by third party, identified by IT dept. etc.

What actions were taken, by whom and why? Give detail of agencies informed and contact person within those agencies.

Name of person completing this form:

Name of setting:

Signature: Date:
Online Safety Incident Log

All online safety incidents must be recorded on the form below. The Senior Designated Person for Safeguarding will be responsible for monitoring incidents regularly, and reporting any concerns or perceived trends to the management team.

<table>
<thead>
<tr>
<th>Date/time</th>
<th>Name of child/practitioner/other</th>
<th>Computer/device</th>
<th>Intentional/unintentional/unknown</th>
<th>Details of incidents</th>
<th>Actions taken/by whom/when/why</th>
<th>Online Incident Log Sheet completed (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Dear [name of parent/carero],

We would like to use a photograph of your child for the following purpose:

__________________________________________________________________________

The period of time this image would be used is from

__________________________________________________________________________

to

After this time, the photograph will be returned or destroyed.
We will not share the photograph with any third party or use the image for anything other than the agreed purpose.
We will not use the photograph for anything which could be considered to be negative in tone, or that may cause offence, embarrassment or distress to the child or family.

Consent:
I have read the above statements, and I agree / do not agree to this image being used.

Signature of parent/carero:

Relationship to child:

Date:

A copy of the photograph referred to in this consent form is attached over-leaf.

Copy of photo consent relates to
Photography Consent Form

We recognise that parents and carers are likely to want to record early years setting productions or special events, and families will value the memories evoked from such images for years to come.

We request that parents and carers sign an Acceptable Use Agreement to cover the taking and use of such images, to ensure that the requirements of the Data Protection Act 1998 are adhered to and the wishes of other parents/carers are respected.

I agree to:

- use recording/photography equipment only in the designated areas agreed.
- use recording/photography equipment on the agreed date and time only.
- respect the rights of other parents, and will not attempt to make any recordings if full parental consent cannot be obtained.
- stand to the rear of the designated area to avoid obstructing the view of others.
- avoid taking unnecessary close-ups of individual children (other than my own child).
- avoid taking any photos which could cause embarrassment or distress.
- stop recording/taking photos on the request of any staff member.
- ensure any photographs or videos taken are for my personal use only.
- not sell, publish or display such images in any form, including uploading of photos on to the internet, in line with Data Protection guidelines.

Name of parent/carer:

Name of child:

Date:

Name of production/special event:

Recording equipment used (delete as applicable):
camcorder / camera / mobile phone / other (please state)
Professional Conduct Agreement

We recognise that practitioners and their managers will use online and digital technologies in their personal and social lives. We do not seek to prevent any practitioner or manager from accessing online technologies however we do ask them to sign a voluntary Professional Conduct Agreement to ensure there is no confusion between their home and professional roles.

Name of practitioner/manager:

I agree that through my recreational use of social networking sites or other online technologies that I will:

- not bring the early years setting into disrepute.
- observe confidentiality and refrain from discussing any issues relating to work, children and young people or parents/carers.
- not share or post, in an open forum, any information that I would not want children and young people, parents/carers or colleagues to view.
- set privacy settings to block unauthorised access to my page and to restrict those who are able to receive updates.
- keep my professional and personal life separate, and will not accept children and young people and parents/carers as ‘friends’.
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of the early years setting.
- either avoid using a profile photograph or ensure it is respectable, and an image I would be happy to share with anyone.
- report any known breaches of the above.

I understand that the completion of this form is optional. However, I voluntarily choose to complete it to safeguard my own professional reputation and that of the early years setting. I understand I am in a position of trust and my actions outside of my professional environment could be misinterpreted by others, and I am conscious of this when sharing information publicly with others.

Signature:   Date:
Acceptable Use Rules for Children

Websites can be fun, but always ask a grown-up before using one.

E-mailing and messaging is good for chat, but talking to strangers is far from that.

Bullying is never right, even online it is wrong to fight.

It is always best to be polite, but don’t talk to anyone who gives you a fright.

Sharing with friends is kind and good; but sharing on the web can be misunderstood.

Friends and family are who you know well; strangers are those you must not tell.

Using a nickname makes you clever, but sharing your real name isn’t ever.

Never be afraid to say something is wrong, asking for help is a sign that you are strong.

(Child, Age 9)
Dear Parent or Carer,

This learning journey will be used to reflect your child’s time at our early years setting. It will include observations of your child at play, photographs and other information. The aim will be to provide you with a continuous picture of your child’s time at our setting. The learning journey will therefore capture your child’s own personal journey, based on their own individual starting point, interests and experiences.

We hope that you will also be able to contribute information to this learning journey, perhaps by including some information and photographs which show what your child enjoys doing at home. This information will help us to ensure that the care, learning and development opportunities we offer your child, compliment those you already offer.

Please remember however, that this learning journey contains personal data that relates not only to your child, but to other children who attend our early years setting. It is likely, for example, that some of the photographs enclosed will capture other children at play. Permission has therefore been obtained to include such information in your child’s learning journey, however it must be remembered that such data is shared for your own personal use only. This means that the information cannot be shared with others, or ‘publicised’ in anyway, without the explicit consent of the parents or carers of those children who may be included. For example, any such photographs cannot be displayed on a social networking site or displayed in a public place.

We appreciate your co-operation in this matter, and request that you sign to acknowledge your agreement.

Child’s name:

☐ I understand and agree with the Learning Journey Trust Statement.
☐ I understand that any data included within my child’s learning journey which relates to another child, is for my information and personal use only.
☐ I will not seek to publicise, display or share such data with others, and will ensure the privacy of other families in doing so.

Parent or Carer’s name:

Signed: (Parent/Carer) Date:
Learning Journey Consent Form

To Name of the child’s parent or carer
Re: Name of child

As encouraged throughout the Early Years Foundation Stage, we will have in place detailed individual learning journeys for all children in our setting, which will document, evidence and monitor their learning and development progress. In all children’s learning journeys, we would like to include photographs of them involved in individual and group play. It is therefore, likely that some of these group photographs will capture other children at play. As the information in these learning journeys will relate to each individual child, it will be treated as personal data, and we therefore ask that you give permission for any photographs of your child involved in group play to be included in other children’s learning journeys. Please note that you will be given the option to view any photographs before they are included in any learning journey, should you request this. As a parent/carer you will also be able to restrict your consent to only allow group photographs (which picture your child) to be included in specific learning journeys. If you would like to restrict your consent to specific learning journeys please state this in writing and return with this consent form. Please also note that should any parent/carer not grant consent to include group images in other learning journeys, relevant images will not be shared across the learning journeys of other children.

Note:
This form is valid for the duration of your child’s time at our early years setting. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your consent at any time.

I consent/do not consent to group photographs being included in other children’s learning journeys

Parent/carer’s signature:

Name: Date:
Key Principles for the Safe Use of ICT in Early Years

Safeguarding is everybody’s business. Children, young people and adults need to be empowered to understand their own individual responsibilities and for working together to keep themselves and others safe from harm.

Training is crucial to effective safeguarding practice – providing an essential understanding of acceptable use, potential risks, signs and indicators of abuse, and the procedures to follow in the event of a concern.

Awareness of risk and effective control measures, rigorous monitoring and supervision are key to creating a safe and secure environment. It is not about prohibiting the use of technologies, such as cameras, but of ensuring, as far as is practically possible, their safe use.

Young children and people learn through the promotion and modelling of positive behaviours, which empower them with the knowledge to recognise, understand and avoid risk – as well as the confidence to report concerns.

Information and communication technology (ICT) provides fantastic opportunities for extending children’s learning. It includes the safe use of technologies such as cameras, phones, game consoles and computers. Remember behaviours pose potential risk not technology.

New technologies are here to stay, and with continuing developments, it is essential to embrace a culture which provides valuable learning experiences and where effective control measures can minimise risk and maximise opportunity.

Gaining knowledge is a powerful tool for all, and it is essential for children to have a full understanding of both the benefits and risks of ICT use – to allow them to build their resilience and prepare them for the ‘digital’ world in which they live, learn and grow.
Effective policies and procedures are essential for outlining rules and guidance to enable ICT to be explored and experienced safely in an environment where acceptable use is promoted and misuse is subject to clear and transparent sanctions.

Security, and safe storage are a priority and personal data, including electronically stored images, must be stored securely with restricted access. Personal technologies should not be used within the workplace for taking, storing or sending such data, including photographs.

Acceptable use policies are essential for enabling, rather than prohibiting, the appropriate use of ICT and for outlining the sanctions for misuse. ICT is a valuable resource when used appropriately therefore the focus must be on enabling rather than preventing its use.

Filtering computer and internet systems provides some control over website access but must be used alongside effective supervision and monitoring procedures. Rigorous control measures are crucial for managing and minimising risk and for ensuring safety.

Enabling and empowering children, young people and adults should be a key aim, avoiding the need to completely restrict or prohibit the use of any form of ICT resource. Clear rules, guidelines, sanctions and monitoring allow for the acceptable and valuable use of ICT.

(Early Years Team, Plymouth)
Online Safety: A Toolkit for Early Years Settings

Other formats

Please ask if you would like this document or information, in another language or accessible format. Please contact: 01752 307450

بطاقة بيرسیه نه گه ر ده خوا زیت نه م به لگه نامه و زانیاریه به هه بیت به زمانیکی تر بان شبازیکی نه گونجا. تکلاه به به ندید به به زماره به ته فوونی 01752 307450

Proszę pytaj, jeśli życzysz sobie Pan/Pani ten dokument lub informacje w innym języku lub w innym formacie dostępu. Proszę telefonować pod nr: 01752 307450

Por favor peça se desear este documento ou informação noutra língua ou em formato acessível. Por favor contacte: 01752 307450

Если бы вы хотели этот документ или информацию на другом языке или в другом доступном формате, пожалуйста свяжитесь по тел: 01752 307450

Eğer bu belge veya bilgiyi başka bir dilde ya da erişilmesi mümkün bir şekilde arzu ediyorsanız, lütfen isteyiniz. Lütfen bu numarayı arayın: 01752 307450