ADDYSG CYMRU
EDUCATION WALES
cenhadaeth ein cenedl | our national mission

Llywodraeth Cymru
Welsh Government

Online safety toolkit for early years practitioners: Guidance

Online safety toolkit for early years practitioners: Guidance

Audience

Early years practitioners working in settings and organisations, both those registered and not registered with Care Inspectorate Wales (CIW); nurseries; day nurseries; play groups; cylchoedd meithrin; out of school clubs; crèches; childminders; parent and toddler groups; Ti a Fi groups; holiday play schemes; and any other provision where practitioners work with children under five.

Overview

The online safety toolkit supports early years practitioners in their everyday use of technology, both as part of the provision and outside of it. It aims to encourage an understanding among practitioners of how children might be supported to safely and responsibly use technology, and promote good practice for keeping children safe. It raises awareness of the role of technology in families and the wider community, as well as highlighting and promoting best practice for managing the risks associated with online technologies.

The toolkit was originally published in 2010, and revised in 2012 and 2017. The 2020 version is the first version specifically produced for Wales and was commissioned by the Welsh Government.

Action required

None – for information only.

Further information

Enquiries about this document should be directed to:
Digital Learning Unit
Digital and Strategic Communications Division
Welsh Government
Cathays Park
Cardiff
CF10 3NQ
e-mail: hwb@gov.wales

Additional copies

This document can be accessed from the Hwb website at hwb.gov.wales/keepingsafeonline

Mae'r ddogfen yma hefyd ar gael yn Gymraeg.
This document is also available in Welsh.

 WG38689 Digital ISBN 978 1 80038 744 7

Contents

Introduction

Introduction

With so much of our lives being online it is essential to teach our children to use the internet safely and promote safe and responsible use of technology.

The Ofcom Online Nation report 2019[1] found that 'children spent much more time online than they did watching television', and estimated the time spent by three and four-year-olds who accessed the internet (52 per cent) to be around nine hours a week. This is a clear indication that media and the internet are entwined in children's lives from a young age. We also know that technology is continuing to evolve at a fast pace and has completely revolutionised education.

Against this backdrop, it is clear why online safety is a key priority for the Welsh Government, as evidenced by our *Online safety action plan for children and young people in Wales 2019*[2], which provides a strategic vision for the work we will take forward to keep children and young people safe online in Wales. There is also a dedicated area on Hwb[3] which hosts news, events and a range of resources on various online safety issues.

It is, of course, important to embrace the exciting opportunities and advances in technology, while also understanding the associated risks.

Access to the most appropriate technologies is important to support learning, and in provisions[4] for children from birth to five-years-old there should be opportunities to 'experience and use a range of media and stimuli including emerging technologies'[5].

The online world provides many opportunities to learn, to be creative and to communicate with each other globally, through both work and play. The online safety toolkit for early years practitioners, which consists of this guidance and 14 supporting documents[6], aims to support practitioners in their everyday use of technology, both as part of and outside the provision. The aim is to encourage an understanding among practitioners of how children might be supported in their safe and responsible use of technology and to raise awareness of the role of technology in families and in the wider community.

We know that children are very influenced by the behaviours of others, and it is important that adults in their lives set a good example for the appropriate and proportional use of technology. Excessive screen time is just one example of a wider range of digital issues that might be considered within the provision and raised with parents/carers.

---

1 www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/online-nation

2 gov.wales/online-safety-action-plan-children-and-young-people

3 hwb.gov.wales/keepingsafeonline

4 'Provisions' refers to all provisions working with children aged up to five. Examples of settings and organisations varying in size which may use the toolkit include both those registered and not registered with Care Inspectorate Wales (CIW), nurseries, day nurseries, play groups, cylchoedd meithrin, out of school clubs, crèches, childminders, parent and toddler groups, Ti a Fi groups and holiday play schemes, and any other provision where practitioners work with children aged under five.

5 Taken from *Foundation Phase Framework* (*Revised 2015*) hwb.gov.wales/curriculum-for-wales-2008/foundation-phase/foundation-phase-framework

6 hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

The toolkit aims to highlight and promote best practice for managing the risks associated with online technologies. Included are exemplar policies and procedures and acceptable use agreement (AUA) templates. The exemplar policies can be considered good practice, although not all aspects of each policy will be applicable or relevant to all provisions. The AUAs should be considered the absolute minimum standard that any provision working with children aged up to five should adopt, including both those registered with Care Inspectorate Wales and unregistered provisions. The toolkit also includes an information sheet which can be displayed in provisions to demonstrate the commitment of staff to encouraging the healthy and positive use of technology.

Having clear policies, ensuring that AUAs are in place and identifying staff training needs are an integral part of keeping children safe online; however, the less formal aspects can also make a difference. This might be learning about what technology children use at home or about their favourite games or apps. Openly discussing the benefits and risks with children and their families is key to promoting safe use.

Nothing is more important than the safety of our children and the toolkit can support provisions in protecting children from illegal and harmful content on the internet in order to ensure that their early experiences with technology are positive.

What is online safety?

What is online safety?

The term 'online safety' is used to describe the safe use of all forms of digital technologies. The aim of online safety should be to reasonably protect all users of such technologies from potential and known risk. Technology itself is only one aspect of this; equally as important are the ways in which technology and behaviours are managed. For safeguarding to be effective, online safety procedures must be clear, agreed, respected and followed.

Effective online safety practice will enable children to use technology safely, whether at home or in the provision. It will empower them to use their acquired skills and knowledge to keep themselves safe, without limiting opportunities for exploration, creativity and innovation.

Everyone has a responsibility to minimise risk, while empowering children, as well as 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 judgements and decisions about acceptable use. It is unrealistic and naïve to think that all risks can be eliminated.

In the report *Safer Children and Young People in a Digital World: The Report of the Byron Review* (2008)[7], Tanya Byron highlights strategic objectives which should be considered when determining the safety of children and young people accessing the internet, including 'increasing resilience'. It is recommended that these objectives are considered when developing online safety policies and procedures.

Safeguarding is everybody's business and ensuring the safety and well-being of children in the provision is paramount. This includes their safety online.

As with any form of safeguarding, it is important that practitioners are aware of the potential risks to children. Some of these risks may include:

- excessive screen time
- prolonged exposure to online technologies, particularly from an early age
- exposure to inappropriate content, images and language, including terrorist and extreme views
- making, taking and distributing indecent images and videos
- online bullying
- grooming
- physical, sexual and emotional abuse
- addiction to technologies and behaviours, e.g. gaming, over-use
- other online harms.

[7] www.iwf.org.uk/sites/default/files/inline-files/Safer%20Children%20in%20a%20Digital%20World%20report.pdf

For practitioners and parents/carers additional risks may also include:

- theft and fraud from activities such as phishing[8]
- pressure from media and targeted advertising
- viruses, Trojans, diallers, key loggers, spyware and other malware[9]
- social pressure to maintain online personas and social networking profiles
- identity theft.

There are also significant implications around data security. This will include how personal data is processed and who has access to it in line with the requirements laid out in the current Data Protection Law applicable to the UK (which includes the EU General Data Protection Regulation (GDPR)).

'Keeping safe online' area on Hwb

The 'Keeping safe online' area on Hwb has been developed to support teachers, parents/carers and learners in the critical area of online safety. It hosts news, events and a range of resources on various online safety issues to help keep learners safe. The teachers' guides (suitable for all education practitioners) and the family guides may prove the most useful in learning more about emerging technologies, safeguarding issues, etc. and to support with raising awareness of these issues with parents/carers.

Equality of opportunity

All children and adults are encouraged to use and benefit from opportunities provided by a range of technologies.

Some children will require additional support and guidance. This may include reminders, prompts and further explanations to reinforce and develop each individual child's existing knowledge and understanding of online safety issues.

Parental involvement

Parents/carers need to be involved fully in promoting online safety within the provision, home and social environment. It is important to regularly share information about online safety issues with parents/carers and be prepared to have discussions about this. The aim should be to encourage a better understanding of the benefits and risks of technology and to help parents/carers to understand what acceptable use means.

Parents/carers should be encouraged to sign AUAs on behalf of, and with, their children (see supporting document 1 (Acceptable use rules for children), supporting document 2 (Exemplar letter for parents/carers about the parent/carer agreement: Acceptable use rules for children) and supporting document 3 (Parent/carer agreement: Acceptable use rules for children) of the toolkit[10]).

---

8 The Hwb Trust Centre provides comprehensive information about data protection and security controls (hwb.gov.wales/support-centre/trust-centre).

9 Malicious software and viruses.

10 hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

Parent/carer permission must be obtained for taking photographs and making video recordings of the children in the care of the provision. Consent should also be obtained for the subsequent use of any images or recordings made (see supporting document 4 (Exemplar letter for parents/carers about taking images/videos) and supporting document 5 (Digital images/video consent form) of the toolkit[11]).

Staff may provide help and advice to parents/carers on the best sources of information on the safe use of technology in the home and/or social environment. Information, advice and guidance is available on the 'Keeping safe online' area on Hwb[12].

Staff should be working in close partnership with parents/carers. They should provide assistance in directing parents/carers to the best sources of advice and information on the safe use of technology in the home and/or social environment.

Managing the risk

The exemplar policies contained in this guidance (see pages 20–47) are intended to be used as templates for a wide range of provisions. These should be amended to meet the needs of each provision.

Maintained provisions must appoint a designated senior person for safeguarding/child protection who is responsible for managing safeguarding/child protection issues and cases as defined in the Welsh Government guidance *Keeping learners safe*[13].

For provisions that provide regulated childcare, the registered person is ultimately responsible for ensuring compliance with the Child Minding and Day Care (Wales) (Amendment) Regulations 2016 which include regulations relating to the safeguarding and welfare of children in their care (see definitions in *National Minimum Standards for Regulated Childcare for children up to the age of twelve*[14]). The registered person must have a child protection policy in place which is understood by all practitioners in the provision. They must also identify a designated member of staff who has received child protection training and is responsible for child protection and liaison with child protection agencies as appropriate.

Non-registered childcare settings may also use the toolkit as best practice within their provisions.

Provisions should have clear and effective policies, practices and infrastructure in place, which are monitored and regularly reviewed to ensure that they continue to meet the ever-changing needs of children in their care.

Where possible, online safety should not be seen as the sole responsibility of one individual. To cultivate a safe environment and a culture where children can use technology safely it is essential to ensure practitioners receive effective online safety training and use clear AUAs.

---

[11] hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

[12] hwb.gov.wales/keepingsafeonline

[13] gov.wales/keeping-learners-safe

[14] gov.wales/national-minimum-standards-regulated-childcare

A safer online environment in early years provisions and childcare

The appointed or identified member of staff (as outlined on page 8) is responsible for applying a duty of care by creating and maintaining a safer online environment for all users in the provision environment.

It will require the need to:

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

Creating a safer online environment is ongoing and ever-changing and will take time to fully introduce into everyday practice. Clear monitoring, evaluation and review of procedures are essential elements for ensuring a safer online learning environment.

Policies and practice

Policies and practice

Many issues surrounding online safety are linked to the behaviour of users – whether children, young people or adults. It is therefore essential that online procedures and practices are developed with the aim of modifying behaviours and promoting acceptable use. Supporting document 14 (Online safety policy prompt sheet) of the toolkit[15] will be particularly useful when developing online procedures and practices as it provides a high-level overview of the key areas for consideration. Consistent strategies should be in place to ensure an effective response to any incidents or allegations of potential misuse.

Online safety should form an integral part of the welfare, learning and development programme for all children. Effective links must therefore be made to key policies and procedures, such as recruitment, induction and safeguarding, and it should be firmly embedded across the curriculum. To be effective, policies and procedures must be rigorous, enforced, monitored and reviewed to ensure they remain fit for purpose.

The exemplar policies in this guidance (see pages 20–47) are intended to help provisions produce a suitable online safety policy document which will consider all current and relevant issues in the context of the provision, linking with other relevant policies, such as the provision's safeguarding, behaviour and anti-bullying policies.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all practitioners are bound. Provisions must, through their Online Safety Policy, meet their statutory obligations to ensure that children are safe and are protected from potential harm. The policy will also form part of the provision's protection from legal challenge, relating to the use of digital technologies.

An effective online safety policy must be tailored to the needs of each provision and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole community. It is suggested that consultation in the production of this policy should involve a wide range of stakeholders.

Due to the ever-changing nature of digital technologies, it is best practice that provisions review their Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Supporting resources to enable online safety within a provision

For a provision based in a school, 360 degree safe Cymru[16], developed by South West Grid for Learning (SWGfL) on behalf of the Welsh Government, is a powerful self-review tool for reviewing online safety procedures. The tool will not only audit current provision, but will also benchmark progress, provide clear advice on how to progress further, manage reports, and help develop and identify future planning and training needs.

The Online Compass[17] self-review tool, is relevant to other provisions and has been written for smaller organisations.

---

[15] hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

[16] To access 360 degree safe Cymru on Hwb, users in provisions/schools should log in to Hwb and click on the link to the 360 tool under Hwb tools.

[17] https://onlinecompass.org.uk

Acceptable use agreements

Acceptable use agreements

Acceptable use agreements (AUAs) are fundamental to risk management. Exemplar AUAs can be downloaded as individual templates (see supporting documents 1, 2 and 3 of the toolkit[18]). These should be considered in conjunction with supporting policies in this guidance as a baseline to minimising risk. In order to maximise impact, however, it will be essential for all areas of policy, procedure and practice to link together, so as to ensure clear, effective and joined-up strategies are fully established and implemented.

Furthermore, it is essential that early years and childcare practitioners and their managers have a clear understanding of what are acceptable and unacceptable behaviours. This should help to ensure the behaviour of users is not open to misinterpretation.

It is clear from the *Keeping learners safe* guidance that it is everybody's duty to ensure that children are protected from potential harm. The involvement of children, young people and parents/carers is vital to the effective and safer use of online technologies. The AUA should therefore inform children and parents/carers of their own responsibilities. The process of developing an AUA should be consultative, taking account of the views of all those involved.

Aim of the AUA

The AUA that provisions develop should aim to:

- safeguard children by promoting appropriate and acceptable use of technology
- outline the roles and responsibilities of all individuals who have access to and are users of work-related technology systems
- ensure all users of technology in the provision environment have an awareness of risk, a clear understanding of what constitutes misuse, and how the strategies employed in response to misuse and responsible use should be implemented.

The AUAs included as supporting documents as part of the toolkit are intended to be used as a template for a wide range of provisions and should be amended to meet the needs of each provision.

Scope of the AUA

The AUA will apply to all individuals who have access to and/or are users of work-related technology systems. This will include children or their parents/carers, practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

While we recognise that children may be too young to give informed consent on their own, 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.

---

[18] hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

Parents/carers and, where applicable, other agencies will be informed of any incidents of inappropriate use of technology (including activity such as distributing racist material, online bullying, grooming, possession of or access to pornography, promotion of terrorism, or breaches of the Computer Misuse Act) that take place on-site, and, where relevant, off-site.

Roles and responsibilities

Safeguarding lead

Those responsible for safeguarding must have relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role should be available at all times, including, where necessary, the use of a designated deputy.

The person responsible for safeguarding/child protection will be required to ensure:

- agreed policies and procedures are implemented in practice
- all updates, issues and concerns are communicated to all users of technology in the provision environment
- the importance of online safety in relation to safeguarding is understood by all users of technology in the provision environment
- the training, learning and development requirements of all staff is monitored and additional training needs identified and provided for
- an appropriate level of authorisation is given to users of technology (not all levels of authorisation will be the same) – this will depend on the position, work role and experience of the individual concerned and, in some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate
- any concerns and incidents are reported in a timely manner in line with agreed procedures
- the learning and development plans of children address online safety
- a safe learning environment including the use of technology is promoted and maintained.

Appointed/identified individual responsible for online safety

This person will have overall responsibility for ensuring that online safety is an integral part of everyday safeguarding practice. This includes ensuring that:

- staff receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures
- clear and rigorous policies and procedures are applied to the use/non-use of personal devices and equipment by all individuals who come into contact with the provision – such policies and procedures should include the personal use of work-related resources
- the AUA is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity
- the use of online technologies are monitored and that monitoring procedures are open and transparent

- allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, including the police where applicable
- effective online safeguarding support systems are put in place, e.g. filtering controls, secure networks and virus protection.

Practitioners and their managers

Practitioners and their managers will ensure:

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

Children

Children should be encouraged to:

- be active, independent and responsible learners, who are engaged, as appropriate to their age, in policy and review
- abide by the AUA
- report any concerns to a trusted adult.

Parents/carers

A copy of an AUA should be provided to parents/carers on enrolment of their child at the provision. This will be reviewed regularly. It is an expectation that parents/carers will explain and discuss the AUA with their child to ensure that it is understood and agreed. Children will also be encouraged to 'sign' the AUA alongside their parent/carer where appropriate. Records of all signed agreements should be kept on file.

Should parents/carers wish to use personal technologies (such as cameras) within the provision environment, practice must be in line with the provision's policies.

Acceptable use by practitioners, their managers and volunteers

Practitioners, their mangers and volunteers 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
- for recording data when appropriate.

All practitioners, their managers and volunteers will be subject to authorised use as agreed by the person responsible for safeguarding/child protection. They should be provided with a copy of the AUA, which they must sign, date and return (see supporting document 7 (Acceptable use agreement for staff and volunteers) of the toolkit[19]). A signed copy should be kept on file.

Authorised users should have their own individual password to gain access to a filtered internet connection. Users are not permitted to disclose their password to others, unless required to do so by law or where requested to do so by the person responsible for safeguarding/child protection. All devices, computers and related equipment that can access personal data should be locked when unattended to prevent unauthorised access.

The use of personal technologies should be defined in the provision's Mobile Devices Policy (see pages 39–42 for an exemplar policy) and is subject to the authorisation of the person responsible for safeguarding/child protection, and such use should be open to scrutiny, monitoring and review.

Online safety incident response

In the event of an allegation of misuse by a practitioner, their manager or volunteer, a report should be made to the person responsible for safeguarding/child protection immediately (see supporting document 8 (Online safety incident log) and supporting document 9 (Online safety incident report sheet) of the toolkit[20]). Should the allegation be made against the person responsible for safeguarding/child protection, a report should be made to a senior manager. Procedures should be followed as appropriate, in line with the provision's Misuse of Information and Communication Technology Policy (see pages 43–47 for an exemplar policy) and/or disciplinary procedures. Should allegations relate to abuse or unlawful activity, Care Inspectorate Wales, the local authority, and/or the police should be notified as applicable (see supporting document 10 (Online safety incident response flowchart) of the toolkit[21]).

Acceptable use by children

AUAs are used to help children and their families understand the behaviour that is expected of them when accessing the internet. This should be shared with the children in an age-appropriate manner such as through the use of images, pictures, posters or discussion activities. Parents/carers should be encouraged to agree to support their child in understanding what is acceptable or unacceptable online.

The AUAs are shared and agreed with children and should be displayed in the provision as a reminder.

---

19 hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

20 hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

21 hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

In the event of misuse by children

It is unlikely that a child in a birth to five-years-old provision would deliberately attempt misuse. If this should occur the provision should regard it as a safeguarding concern and use the normal safeguarding procedures. They should also:

- follow the guidance provided in the provision's Misuse of Information and Communication Technology Policy (see pages 43–47 for an exemplar policy)
- inform the parent/carer of the issue
- discuss with the child why this has happened
- provide support and guidance to the child.

In the event that a child accidentally accesses inappropriate material, it must be reported to an adult immediately. Appropriate action should be taken to hide or minimise the window. The device should not be switched off, nor the page closed, in order to allow investigations to take place. A conversation should take place with the child and with the parent/carer. Appropriate action should be taken after the incident to ensure that the situation cannot occur again in the future.

Acceptable use by visitors, contractors and others

All guidelines in respect of acceptable use of technologies must be adhered to by any visitors or contractors.

Links to other policies

Relevant policies, such as the Safeguarding Policy, Behaviour Policy or Health and Safety Policy in place at the provision, should be referred to when dealing with any incidents that occur as a result of the intentional or unintentional misuse of technology.

Any allegations of abuse or other unlawful activity should be reported immediately to the person responsible for safeguarding/child protection, who will ensure procedures outlined in the provision's Safeguarding Policy are followed with immediate effect.

It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed online or offline.

Other online policies

The AUA should be clearly linked to the provision's:

- Internet Policy
- Digital and Video Images Policy
- Mobile Devices Policy
- Misuse of Information and Communication Technology Policy.

Exemplar policies for the above can be found in the 'Developing an online safety policy document' section of this guidance on pages 20–47.

Developing an online safety policy document

Developing an online safety policy document

The following exemplar policies are intended to be used as templates for a wide range of provisions to aid in the development of an online safety policy document, linking with other relevant policies. Not all aspects of each exemplar policy will be applicable or relevant to all provisions and therefore should be amended to meet the needs of each provision. As part of the development process, provisions should engage with a wide range of stakeholders to ensure the policy is accepted and owned by the whole community.

The exemplar policies in this section include:

- Internet Policy (see pages 20–25)
- Digital and Video Images Policy (see pages 26–37)
- Mobile Devices Policy (see pages 38–41)
- Misuse of Information and Communication Technology Policy (see pages 42–46).

There are a range of titles for identified or appointed safeguarding lead. As such, the umbrella term 'the person responsible for safeguarding/child protection' is used throughout the exemplar policies, but can be amended as required.

The online safety policy document will ensure that provisions meet their statutory obligations to ensure that children are safe and are protected from potential harm online. The policy will also form part of the provision's protection from legal challenge, relating to the use of digital technologies.

Due to the ever-changing nature of digital technologies, it is best practice that provisions review their online safety policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Exemplar Internet Policy

This exemplar policy is intended to be used as a template for a wide range of provisions and should be amended to meet the needs of each provision.

Introduction

The internet is part of everyday life. Knowledge and experience of technology should be considered as essential. Developmentally appropriate access to the internet in the early years contributes significantly to children's enjoyment of learning and development.

Children learn most effectively where they are given managed access to the internet and control of their own learning experiences; however, such use carries an element of risk. Practitioners, their managers and volunteers, alongside parents/carers, should make children aware of the potential risks associated with online technologies. This empowers them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Aim

The Internet Policy aims to outline safe and effective practice specific to the use of the internet. It provides advice on acceptable use and effective measures to enable children and adults to use the internet and its wealth of resources in a safe way.

It applies to all individuals who have access to and/or are users of the internet connection provided by the provision. This includes children, parents/carers, practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

It also applies to internet access through any means, e.g. computers, tablets, mobile devices and gaming devices.

Responsibilities

The person responsible for safeguarding/child protection is responsible for online safety, and manages the implementation of the Internet Policy. They 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 users of the internet in the provision environment are aware of the procedures that must be followed in the event of a potentially unsafe or inappropriate online incident taking place
- the recording, monitoring and filing of reports in the event of a potentially unsafe or inappropriate online incident – this should include the creation of an incident log which should be used to inform future online safety practice
- all necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring

- regular meetings, if appropriate, with senior managers to discuss current issues, review incident reports and filtering/change control logs
- effective training and online safety advice is delivered and available to all staff and volunteers – this includes advisory support to children and parents/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, including reporting to the police, where necessary.

(Details on responsibilities can be found in the 'Acceptable user agreements' section of this guidance (see page 13).)

Managing online access

Password security

Maintaining password security is an essential requirement for all staff in the provision environment, particularly where they have access to personal information. A list of authorised users should be maintained, and access to sensitive and personal data should be restricted.

Staff will be responsible for keeping their passwords secure and should ensure they are regularly updated. All users in the provision environment should have strong passwords. For more information see the Password Management and Security Guide[22] from SWGfL.

Passwords should not be shared. Where children have their own passwords there should be the option to reset if lost or forgotten.

All internet-enabled devices should be set to 'time-out' the current user session if they become idle for an identified period. All users in the provision environment must 'log out' of their accounts if they need to leave a device unattended.

If users become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the person responsible for safeguarding/child protection.

Internet access

Internet access for all users in the provision environment should be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution should 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. Control measures should be put in place where appropriate to manage internet access and minimise risk.

[22] https://swgfl.org.uk/resources/password-management-and-security-guide

Measures should include:

- secure broadband or wireless access[23]
- secure e-mail accounts[24]
- regularly monitored and updated virus protection
- a secure password system
- an agreed list of assigned authorised users with controlled access and defined responsibilities
- clear AUAs
- effective audit, monitoring and review procedures.

Online activity should be monitored to ensure access is given to appropriate materials only. This may mean an adult physically observing the child when using technology, or in large provisions the implementation of a software monitoring solution.

Internet-connected devices should be sited in areas of high visibility, which will enable children and adults to be closely supervised and their online use to be appropriately monitored.

If a child accidentally accesses inappropriate material, staff must report it to the person responsible for safeguarding/child protection immediately. Appropriate action should be taken to hide or minimise the window. The device should not be switched off, nor the page closed, in order to allow investigations to take place. All such incidents must be reported to the person responsible for safeguarding/child protection, who must ensure a report of the incident is made and that any further actions deemed necessary are taken.

All staff should be made aware of the risks of connecting personal mobile devices to work-related systems.

Should it be necessary, the download of files or programmes to any work-related system should be effectively managed and monitored.

All users in the provision environment are responsible for reporting any concerns encountered using online technologies to the person responsible for safeguarding/child protection.

Online communications

All official online communications should occur, where possible, though secure filtered e-mail accounts. Provisions should be aware that free, web-based e-mail services are not considered secure for personal data and their use could put the provision at risk.

All e-mail correspondence should be subject to scrutiny and monitoring.

---

[23] The Digital Infrastructure Support area on Hwb provides comprehensive information to help organisations manage their digital environment (hwb.gov.wales/support-centre/digital-infrastructure-support).

[24] The Hwb Trust Centre provides comprehensive information about data protection and security (hwb.gov.wales/support-centre/trust-centre).

All users in the provision environment are expected to write online communications in a polite, respectful and non-abusive manner. The appropriate use of emoticons should be encouraged.

It is strongly recommended that a filtered internet connection is used to monitor and prevent offensive material or spam. If, on rare occasions, security systems are not able to identify and remove such materials, the incident should be reported to the relevant senior manager immediately.

Communication between adults and between children and adults, by whatever method, should take place within clear and explicit boundaries. This includes the wider use of technology such as mobile devices, text messaging, social networks, e-mails, digital cameras, videos, webcams, websites and blogs.

When using digital communications, staff and volunteers should:

- ensure that they act in accordance with any legal requirements, e.g. data protection laws/policy
- only make contact with children for professional reasons
- only make online contact in accordance with the policies and professional guidance of the group
- not share any personal information with a child, e.g. should not give their personal contact details to children including e-mail, home or mobile telephone numbers
- not request, or respond to, any personal information from the child, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised
- ensure that all communications are transparent and open to scrutiny
- be careful in their communications with children so as to avoid any possible misinterpretation
- ensure that if they have a personal social networking profile, details are not shared with children in their care (making every effort to keep personal and professional online lives separate)
- not post information online that could bring the provision into disrepute
- be aware of the strategies employed in response to misuse that may be applied for breaches of policy related to professional conduct
- only use (wherever possible) official equipment or systems to communicate with children.

All users in the provision environment are advised not to open e-mails where they do not know the sender or where the format looks suspicious, and should be extremely cautious when opening any attachments.

Children should be enabled to use online technologies as relevant to their age and development. Access to online communications should always be monitored by a supervising adult.

Managing mobile and emerging technologies

Emerging technologies can offer potential learning and development opportunities. Their use should be risk assessed before use by children and young people. Where necessary, further training and guidance should be provided to ensure appropriate and safe use of any new technologies.

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

Many of these devices will be equipped with internet access, GPS, cameras, and 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, while maximising the opportunities for children to access such resources.

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

Access to social networking sites should be carefully managed within the provision, and children will only be permitted to use moderated, child-focused sites under supervision. Staff are not permitted to use work-related technologies for personal access to social networking sites. Provisions may wish to refer to the 360 degree safe Cymru Social Media Policy[25] designed for schools/colleges which covers both personal and organisation use.

All users in the provision environment should be encouraged to think carefully about the way information can be added and removed from websites by themselves and others.

Children should be taught to think carefully before placing images or videos of themselves online and to be aware of details within images or videos, such as badges, which could reveal personal and background information. Users should consider the risks of posting images or videos online owing to the permanency of online material.

Children must always be reminded not to give out or post personal details online, particularly information which could identify them or provide information that would contribute to their personal profile.

Children should be educated on how to set and maintain web profiles to appropriate privacy levels and how to deny access to unknown individuals.

[25] hwb.gov.wales/playlists/view/2827fbc0-09b9-453e-a9f6-50935845812e/en/13

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

Staff are also likely to use social networking sites in their recreational time on their own personal devices. This form of activity is not to be discouraged. However, practitioners must adhere to a 'professional conduct agreement' (see supporting document 13 (Voluntary professional conduct agreement) of the toolkit[26]). The use of such sites should not compromise professional integrity or bring the provision into disrepute. The adding of children and/or parents/carers as 'friends' to social networking sites should be avoided.

Social networking sites and mobile technologies can be used for negative and anti-social purposes. Online bullying, for example, is unacceptable, as is any other form of bullying, and effective, consistent strategies employed in response to misuse must be in place to deal with such concerns. Any known or suspected incidents must be reported immediately to the person responsible for safeguarding/child protection.

[26] hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

Exemplar Digital and Video Images Policy

This exemplar policy is intended to be used as a template for a wide range of provisions and should be amended to meet the needs of each provision.

Introduction

The use of stand-alone cameras and devices with cameras should be considered an essential and integral part of everyday life. As such, children and staff should be encouraged to use such technology in a positive and responsible way.

It is recognised, however, that digital technology has increased the potential for images and videos to be misused and inevitably there will be concerns about the risks to which children may be exposed.

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

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

Aim

The Digital and Video Images Policy aims to ensure safer and appropriate use of images and videos through agreed acceptable use procedures. This is in line with legislative requirements and aims to respect the rights of all individuals.

Scope

The Digital and Video Images Policy will apply to all individuals who have access to and/or are users of work-related photographic and recording equipment. This will include children, parents/carers, practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

The Digital and Video Images Policy applies to the use of any device with a camera. This includes smartphones, tablets and portable gaming devices with inbuilt cameras, as well as other forms of digital technology and resources for storing and printing images.

Responsibilities

The person responsible for safeguarding/child protection is responsible for ensuring the acceptable, safe use and storage of all camera technology, images and videos. This includes the management, implementation, monitoring and review of the Digital and Video Images Policy.

(Further details on responsibilities can be found in the 'Acceptable user agreements' section of this guidance (see page 13).)

Legislative framework

This policy complies with the requirements of the Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), Freedom of Information Act 2000, and other relevant laws regarding the taking and use of images and videos of children.

All images and videos will be used in a manner that meets the requirements of the seven Data Protection Principles.

This means that images and videos will have:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability
- adequate protection if transferred to other countries.

Most organisations that process personal data must register under UK Data Protection Laws (which include obligations required under EU General Data Protection Regulation (GDPR)) with the Information Commissioner's Office (ICO). Some provisions may be exempt. For further details please visit the ICO website[27] or their helpful guidance on taking photographs in schools[28].

Code of conduct

All staff must ensure that the policy and procedures included herein are adhered to at all times. The Digital and Video Images Policy should be considered in conjunction with the provision's AUA, Data Protection Policy, and the Misuse of Information and Communication Technology Policy.

The use of cameras and other photographic and recording equipment should be authorised by the person responsible for safeguarding/child protection. It must be recognised that individuals may be given different levels of responsibility in terms of authorised use.

Wherever practical, cameras and other photographic and recording equipment should be designated for work-related purposes only. Personal photographic and recording equipment should not be used to take digital imagery or recordings in the provision. If such use is allowed, authorisation must be obtained from the person responsible for safeguarding/child protection and all relevant details of use should be recorded.

---

[27] https://ico.org.uk

[28] https://ico.org.uk/your-data-matters/schools/photos

The transferring of images and videos via unprotected USB sticks, unfiltered web mail or via unprotected mobile media should be prohibited. If remote access is given to servers or systems where images and videos are to be stored, access will only be given as authorised by the person responsible for safeguarding/child protection. Any personal data stored on servers outside of the UK must comply with standards designated by UK Data Protection Laws (which include obligations required under the EU GDPR).

The person responsible for safeguarding/child protection must reserve the right to view any images and videos taken and/or to withdraw or modify an individual's authorisation to take or make images and videos at any time. Staff must ensure that all images and videos are available for scrutiny and be able to justify any images and videos in their possession.

The person responsible for safeguarding/child protection is responsible for ensuring the safe storage of all images and videos, in accordance with the Digital and Video Images Policy and in accordance with data protection laws concerning the appropriate storage of personal data.

Staff have a duty to report any concerns relating to potential misuse. Clear whistleblowing procedures should be in place. An anonymous reporting system may also be promoted and used to facilitate this process. Staff may wish to use Crimestoppers[29] to anonymously report criminal activity.

Consent

Consent (which is one of the lawful bases to use data) under UK Data Protection has changed. Consent is defined in Article 4(11) of the EU GDPR as:

> 'in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data'.

This means that where a provision is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but provisions should consider the capacity of children to freely give their informed consent.

Provisions should only use consent if none of the other lawful bases is appropriate. If they do so, they must be able to cope with people saying no (and/or changing their minds), so it's important that they only use consent for optional extras, rather than for core information the provision requires in order to function. For example, consent would be appropriate for considering whether a child's photograph could be published in any way. However, if the provision requires learner details to be stored in a management information system (MIS), it would not be appropriate to rely on consent if the child cannot opt out of this. In this case, provisions could apply the public task lawful base.

---

[29] https://crimestoppers-uk.org

Procedures

Only consent provided by a parent/carer with parental responsibility is to be accepted. Friends or other relatives will not be able to give such consent.

The child's parent/carer has the right to refuse or withdraw their consent at any time.

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

Images or videos of children who no longer attend the provision should not be used, unless specific consent has been obtained to cover this extended period. Generally, consent to use images and videos will lapse should a child leave the provision.

Images and videos

It is recognised that children could be exposed to potential risk should images or videos be misused, including:

- the making, taking and distribution of inappropriate and indecent images or videos
- 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).

It should be remembered that such incidents occur rarely and it should also be understood that detailing such concerns will often raise further anxieties and will make many individuals feel uncomfortable. However, it must be acknowledged that the first step towards minimising any danger is to have a fuller understanding of what constitutes a risk and what behaviours may compound it.

Protective and precautionary measures should therefore be considered when taking, making or using images or videos of children, and practitioners and their managers should be expected to agree and sign up to an AUA.

Procedures

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

Sensitivity must be shown to any child who appears uncomfortable, and the potential for misinterpretation must be recognised. Images or videos should therefore not be taken of any child against their wishes.

The taking or making of images or videos of a child in a one-to-one situation with an adult must be avoided whenever possible, unless there is an agreed, specified reason for doing so. It must be recognised that the context of such situations is likely to be perceived as sensitive and the use of cameras will be seen as intrusive and open to misinterpretation. It should be recognised that this may leave both the adult and child in a vulnerable position and is therefore not accepted practice.

Images or videos should not be taken of any child if they suffer an injury, whether it is accidental or non-accidental. This will be deemed a misuse of power which will potentially cause the child to become distressed or to feel humiliated. Where necessary, medical help should be sought, and in the case of a suspected non-accidental injury, the provision's Safeguarding Policy should be implemented with immediate effect.

Images or videos which may cause distress, upset or embarrassment must not be used.

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

The taking or making of images or videos in sensitive areas of the provision, e.g. toilet cubicles and changing areas, are not permitted.

It should be ensured that a child's full name or any other identifying information does not appear in any caption or accompanying text alongside their image, e.g. on displays, documentation panels and name cards. Particular care should be taken where such images or videos are likely to be viewed by others, including the general public.

Consideration should always to be given to where images or videos are published. Parents/carers should respect the rights of other parents/carers when taking photographs or videos of their child at a group event. It is important that they are made aware of expectations of how images and videos may be used, i.e. that they should not share any image(s)/video(s) of other children publically on social media without the consent of the parents/carers of the other children in the image(s)/video(s).

Use of images and videos of children by the media

Journalists, under the Independent Press Standards Organisation's (IPSO) Editors' Code of Practice, are normally allowed to use imagery and other content from social media where there are no privacy settings protecting them and they do not show anything private. But if the image or video intrudes on grief, privacy or a child's welfare then consent must be sought – in the case of a child, from their parent/carer.

There may be occasions where media companies are invited to a planned event to capture images and/or videos of the children who take part. In these situations it is usual for consent to be collected from the parents/carers for the taking, processing and publication of the images and videos. In this context, the media organisation will be acting as the data controller (and possibly the processor too) so it is reasonable to expect them to manage the collection of consent.

Generally, parents/carers will take pride in 'press cuttings'. For the majority, this pride will often outweigh any fears about the image, video and/or information being subject to misuse. However, some parents/carers may object to information about, and images/videos of, their own children being published. As a result, it should be ensured that parent/carer consent has been sought before the press is given any access to

children. If a parent/carer chooses not to give permission for their child to be involved in such circumstances, this right must be observed at all times. However, care should be taken to ensure that the child is not isolated or disadvantaged by any consent decision made.

Procedures

The manner in which the press will use digital media is controlled through relevant industry codes of practice as well as the law. In this way a check is put on the potential improper use of images and videos of children by the press. Additional checks should also be carried out by the person responsible for safeguarding/child protection. This ensures that broadcasters and press photographers are made aware of the sensitivity in respect of detailed captioning, one-to-one interviews, and close-up digital media capture.

Where media organisations are invited to celebrate an event, every effort should be made in advance to ensure that their requirements are able to be met. Where, for example, a newspaper is invited to take photographs of children, it is usual practice for names to be provided. Newspapers will be very unlikely to print anonymous photographs. The provision may request that only first names are used. However the provision should make it clear to parents/carers that responsibility and liability cannot be held for the actions of a third party organisation, should they choose not to abide by any of those requests.

The identity of any media representative must always be verified. Access will only be permitted where the event is planned, and where media are specifically invited to attend. No authorisation will be given to unscheduled visits by the media under any circumstances. In the event that the media should turn up uninvited, for reasons beyond the control of the provision, every reasonable effort will be made to ensure that children and parents/carers are protected from any press intrusion.

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

Use of a professional photographer[30]

It should be ensured that any professional photographer engaged to record events is prepared to work according to the terms of the Digital and Video Images Policy 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 2018 and GDPR.
- Photographers will only be used where they guarantee to act appropriately to prevent unauthorised or unlawful processing of images or recordings, and will insure against accidental loss or destruction of, or damage to, personal data.

[30] The term 'photographer' is used in this guidance, but these guidelines are applicable to other professionals in this field, including videographers.

Procedures

Photographers should be expected to demonstrate that they have agreed to ensure:

- compliance with the Data Protection Act 2018 and GDPR
- images and recordings are only used for a specified purpose and will not be used in any other context
- images and recordings will be deleted from all storage devices after they are no longer required and within a specified retention period
- images and recordings are not disclosed to any third party unless it is a specific requirement to do so in order to fulfil the requirements of the agreement, such use will also be subject to parent/carer permission.

Care should be taken when choosing photography agencies and/or professional photographers.

Details of any checks regarding suitability, which may include evidence of Disclosure and Barring Service (DBS) checks, will be requested. Photographic identity should be checked on arrival. If there are any concerns in respect of the authenticity of any photographer, entry will be refused and such concerns should be reported.

Photographers should be treated as any other visitor. As such, appropriate levels of supervision should be in place at all times. This will ensure that no unsupervised access to children is given.

Children taking photographs and videos of each other

Children may on occasion be given the opportunity to take photographs and videos of each other and their surroundings. This practice will often occur in many different environments and for most children it will be normal practice to take photographs and/or videos to record a trip or event. Children may also be given access to cameras or recording devices within the provision environment to support their learning and development needs. These activities should be encouraged in a safe and enabling environment.

Procedures

Staff should discuss and agree age-appropriate acceptable use rules with children regarding the appropriate use of cameras and recording devices.

Parents/carers taking photographs and videos

Parents/carers are entitled to take photographs or videos of their own children within the provision, e.g. during school shows.

However, the right is reserved to refuse parents/carers the opportunity to take photographs and make videos.

The provision will publish guidance or announce details of the photography and video guidelines prior to the start of the event (see supporting document 6 (Exemplar photography/recording agreement for use by provisions) of the toolkit[31]).

[31] hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

Procedures

Parents/carers should complete a photography and video AUA if they wish to take or make any photographs or videos within the provision. Authorised use will only be permitted on agreed dates and times, and within designated areas of the provision.

Parents/carers will only be permitted to take photographs or make videos of any event for their own personal use. The use of such images and videos for any other purpose, without express permission, should not be allowed.

The publishing of images and videos on social media should be restricted to only close friends and families. Where wider sharing is desired, consent must be obtained from the parents/carers of all other children in the image or video before sharing.

Parents/carers who are authorised to use photographic or recording equipment should be encouraged to be mindful of others when making and taking such images and videos. This ensures minimum disruption to other parents/carers during any event or production. The right to withdraw consent will be maintained and any images or recordings must be open to scrutiny at any time.

The provision will recommend that parents/carers check privacy settings on social media accounts to understand who can view any images or videos they share.

Closed-circuit television (CCTV)

Closed-circuit television (CCTV) may be used:

- to control access
- to monitor security
- for site management, e.g. 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 practitioners, e.g. in the vicinity of toilets (but not in toilet cubicles)
- for agreed and arranged focused observations of children and practitioners and their managers
- to act as an effective deterrent to prevent crime and to discourage trespass.

Procedures

CCTV cameras capture images or recordings of individuals meaning that the use of CCTV is covered under the Data Protection Act 2018 and GDPR. The Information Commissioner's Office (ICO) has published a CCTV code of practice[32] which provisions would be well advised to review and ensure any CCTV systems are implemented in accordance with this code.

All areas which are covered by CCTV must be well signposted, and notifications should be displayed so that individuals are advised before entering such a vicinity.

If CCTV is used within the provision, the manufacturer's instructions and data protection and information sharing guidelines should be followed at all times. This should include the appropriate storage and disposal of all recordings.

[32] https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Recordings should 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 should be erased before disposal.

Regular auditing of any stored recordings should be undertaken by the person responsible for safeguarding/child protection.

Every effort will be made to avoid inadvertently taking inappropriate recordings and therefore cameras will be placed and positioned sensitively. No cameras should be pointed directly at toilet cubicles or any other sensitive areas within the provision.

Recordings taken outside of operational hours should be erased in accordance with the procedures previously identified.

Webcams

Parent/carer consent must be obtained before webcams are used within the provision. Before seeking such consent, full details of why a webcam is to be used should be provided. This should also include information on the use of the recording/live video, who is to be given authority to view them, and the security measures which will be implemented to prevent unauthorised access.

Procedures

The regulations which apply to webcams regarding signage should be the same as for CCTV.

If filming takes place, children, parents/carers and staff should be consulted. Written consent should be obtained from all parents/carers.

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

(For guidance on mobile devices refer to the Mobile Devices Policy.)

Websites

The posting of images or videos on the provision's website or on a public website may raise particular issues and concerns.

There is a risk that such images or videos could be subject to manipulation and circulation without consent or even knowledge. The risk that children could be exploited in some way after having their image or video displayed should also be acknowledged.

Procedures

Caution should be taken when permitting the publication of images or videos of children taken at the provision. Names and images should not be used together on any public site and clear consent must be obtained for the use of any image or video.

The use of secure learning platforms should, however, be promoted. Images or videos of children can be securely posted and such use is therefore encouraged. Uploading of images or videos to these sites will be covered by the photography and video AUA.

Children's progress records

Many practitioners and their managers track children's progress and have a system for channelling the wealth of information gathered about individual children into a manageable summary. Detailed individual activity in a particular context, photographs/videos and special moments all combine to form these records. Such records may be known by a variety of terms, such as 'children's progress records', and are used to document and monitor the individual learning and development progress of each child in the early years age group (from birth to five-years-old).

Procedures

The information contained within each record relates to an individual, identifiable child; therefore, it must be treated as personal data. This means that such information is protected as laid out in UK Data Protection Laws and should be included in a data protection impact assessment which identifies the data protection risks and enables provisions to mitigate these.

A code of practice statement may be used to protect and promote the welfare and individual rights of children. Details of this code of practice will be included on a Child's Progress Record Statement. It will also be displayed on the front cover of all records.

Consent must be obtained from parents/carers if their child is photographed or recorded among a group of children, or if the image/video is included in a record belonging to another child.

Where possible, therefore, appropriate consent should be requested from parents/carers for group images or videos to be included in the progress records of other children. Parents/carers should also be permitted to restrict their consent. This may mean that group images/videos can only be included in specified progress records, e.g. those which belong to close friends. If it is not possible to obtain consent, the relevant image/video should not be shared across the progress records of other children.

Individual progress records, constructed by practitioners and their managers, are provided for the benefits of the individual child and their parents/carers. Parents/carers should, therefore, be given the responsibility for choosing what to do with any personal data contained in the progress record, once it is in their possession. However, parents/carers must be made aware that they are not permitted to 'publicise' another child without the express agreement of the parent/carer concerned. Parents/carers must therefore be reminded that they must not share, distribute or display those images or videos without relevant authorisation and consent from the parents/carers of all children captured in any of the images or videos.

Professional Learning Passport

During training, practitioners may be required to compile portfolios or passports which will be used to document and evidence their own learning. Part of this documentation may include images or videos of the practitioner working alongside children participating in various activities.

The person responsible for safeguarding/child protection has a duty of care to ensure that practitioners act responsibly in compiling the images or videos included in training portfolios. Practitioners should therefore be monitored in their taking, making and use of such images or videos. All images and videos should be subject to scrutiny and regular audits should be carried out to ensure all relevant policies and procedures are adhered to.

Procedures

The person responsible for safeguarding/child protection should oversee the compilation of images and videos which are used by practitioners when completing training portfolios. Any images or videos which are deemed unsuitable for any reason should not be included.

If images or videos are considered inappropriate, the person responsible for safeguarding/child protection should ensure the provision's Misuse of Information and Communication Technology Policy is applied.

Displaying images and videos

It should be ensured that still images (including those which are displayed digitally) and videos depict children in an appropriate way. The identity of individual children should also be protected. Particular caution should be taken where images or videos are displayed in a public place (the definition of a public place includes any areas where parents/carers, members of the public and visitors are given access).

Procedures

Increased sensitivity and security procedures should be observed when digital displays are used. The positioning of these should be considered, as they are often displayed in the most public areas of the provision, such as the reception.

Storage and disposal

Images and videos should be stored and disposed of securely. The aim is to prevent unauthorised access, ensure confidentiality and protect identity. All images and videos should be stored and disposed of in line with the Data Protection Act 2018 and GDPR.

Procedures

Images or videos should not be kept for longer than necessary. The person responsible for safeguarding/child protection should ensure that all images and videos are permanently wiped from memory cards, computer hard drives and portable drives or other relevant devices once the images or videos are no longer of use or consent has expired.

If images and videos 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 should be stored securely and access restricted.

Images and videos should not be stored on portable storage devices for any longer than is necessary.

Security measures should be the same as those that apply to any personal data.

All images and videos should remain in specified and data protection compliant storage, unless prior explicit consent has been given by the registered person.

Images and videos should be disposed of when no longer required or if consent has expired. They should be returned to the parent/carer, deleted, wiped or shredded as appropriate. Copies should not be taken of any images or videos without relevant authority and consent from the person responsible for safeguarding/child protection and the parent/carer.

A record of all consent details should be kept on file. If permission is withdrawn at any time, all relevant images and videos should be removed and disposed of. The record should be updated accordingly.

Security

All images and videos should be handled as personal data and deemed to be of a sensitive and confidential nature. It should be recognised that damage or distress could be caused if security is breached.

The person responsible for safeguarding/child protection is responsible for ensuring that all information is handled appropriately and securely. If there are any concerns over breaches of security, the person responsible for safeguarding/child protection and/or the registered person are required to take action as appropriate. All such incidents should be recorded, reported and acted upon.

Procedures

Security procedures should be monitored and reviewed regularly.

A data protection impact assessment should be carried out for all processing activities and risks managed to an acceptable residual level.

Under the Data Protection Act 2018, reasonable steps must be taken to ensure the reliability and suitability of any individual who has access to personal data.

To this effect, effective safer recruitment procedures should be applied. Rigorous and regular checks should also be undertaken to ensure the ongoing suitability of all new and existing practitioners and their managers. All relevant checks must be completed before any new employee, volunteer or student on a work placement is given access to children and/or their personal data.

All practitioners are required to follow confidentiality and information-sharing procedures, which must be agreed to at the time of induction.

The following aspects of security are to be managed accordingly.

- Physical security – effective measures should be put in place to ensure physical security and to protect against theft, including that of laptops, computers, mobile devices, cameras, and any personal data, including images and videos.
- Digital security – stringent measures should be implemented to ensure digital security. Awareness should be raised in respect of technological advancements which could put online systems at risks. Security should be updated as and when required.

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

Exemplar Mobile Devices Policy

This exemplar policy is intended to be used as a template for a wide range of provisions and should be amended to meet the needs of each provision.

Introduction

Mobile devices have become more sophisticated over recent years and will continue to evolve, allowing access to new content and services.

Mobile devices allow high-speed methods of communication, which can provide security and reassurance. As with any other form of technology there are associated risks.

Children should be encouraged to understand such risks to enable them to develop the appropriate strategies which increase their resilience and help to keep them safe.

Acceptable use and management of mobile devices is applied through the Mobile Devices Policy, which should be agreed by all service users. The personal use of mobile devices should be limited to specific times and places as laid down in the Mobile Devices Policy.

Aim

The aim of the Mobile Devices Policy is to protect children from harm, by ensuring the appropriate management and use of mobile devices by all individuals who come into contact with the provision.

Children should also 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.

This should be achieved through balancing protection and potential misuse. Alongside the potential risks, mobile phones continue to be effective communication tools. This in turn contributes to safeguarding practice and protection.

Scope

The Mobile Devices Policy applies to all individuals who have access to and/or are users of personal and/or work-related mobile devices within the broadest context of the provision environment. This will include children, parents/carers, practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

Policy statement

It is recognised that the enhanced functions of many mobile devices gives cause for concern, with the potential for misuse. Examples of misuse might include the taking and distribution of indecent images, exploitation and bullying.

Such misuse will have a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not exclusive to children, so the needs and vulnerabilities of all must be respected and protected.

It may be difficult to detect the use or misuse of mobile devices. Their use therefore needs to be effectively managed to minimise the potential for misuse.

Designated 'mobile-free areas' should be situated within the provision, and signs to this effect should be displayed throughout. The areas which should be considered most vulnerable include:

- sleep areas
- relaxation areas
- toilets and cloakrooms
- bathrooms.

In home-based settings, signs may not be appropriate, but it should be made clear to all that images or videos should not be taken in vulnerable areas.

Code of conduct

A code of conduct should aim to create an informed workforce, who will work together to safeguard and promote positive outcomes for the children in their care.

Practitioners and their managers should:

- 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.

Staff and adult use of personal mobile devices in the provision should be restricted to staff-only areas unless pre-arranged in exceptional circumstances. This should be notified to and agreed by all adults who come into the provision.

Procedures

Clearly defined policies and procedures help to ensure effective safeguarding practices which protect children from harm and exposure to behaviours associated with misuse. Care should be taken to ensure that mobile devices do not cause unnecessary and/or unsafe disruptions and distractions in the workplace.

Acceptable use and management of mobile devices should be agreed by all service users. There should be clear expectations and agreement about when and where personal use of mobile devices is allowed. Safe and secure storage facilities should be made available to staff to store personal mobile devices, as necessary.

The recording, taking and sharing of images, video and audio on mobile devices must conform to the guidance specified within the Digital and Video Images Policy. Such authorised use should be monitored and recorded. All mobile device use should be open to scrutiny and the person responsible for safeguarding/child protection may withdraw or restrict authorisation for use at any time if it is necessary.

Staff should not use their own personal mobile device for contacting children and/or parents/carers unless it is an emergency.

All adults, including parents/carers, visitors and contractors should be advised that their mobile devices are not to be used in designated mobile-free areas. If it is necessary for mobile phone calls and/or texts to be taken or made, any unnecessary disturbance or disruption to children must be avoided.

Parents/carers are encouraged to photograph and/or record their child at special events, but are expected to support the provision in keeping children safe. Parents/carers should respect the rights of other parents/carers when taking photographs or videos of their child at a group event. It is important that they are made aware of expectations of how images and videos may be used, i.e. that they should not share any image(s)/video(s) of other children publically on social media without the consent of the parents/carers of the other children in the image(s)/video(s).

All individuals who bring personal devices into the provision must ensure that they hold no inappropriate or illegal content.

Work mobile devices

Work mobile devices should be clearly labelled as such.

The use of a designated work mobile device should be promoted as:

- an effective communication tool, enabling text, e-mail 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
- the specified device for taking images and/or videos of children while away from the provision.

Effective security procedures should be put in place to safeguard against potential misuse. Only authorised individuals should have access to work mobile devices, which should be password protected, and stored securely when not in use.

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

Where the use of a separate work mobile device is not possible, extreme care should be used to ensure that there is a distinction between personal and business use of the device. This might include the use of a separate app only used to communicate with parents/carers, or restricting personal social media use to another mobile device, or logging out of personal accounts during work.

Driving

Staff who are required to drive on behalf of the provision must ensure any work and/or personal mobile devices are switched off while driving.

When driving on behalf of the provision, practitioners and their manager should not make or take a phone call, text or use the enhanced functions of a mobile phone. This also applies to the use of hands-free and wireless connections, which can be a distraction rather than a safer alternative.

Safe storage

A designated safe and secure area should be made available to staff for the storage of personal mobile devices during the working day.

Staff should recognise that any personal mobile devices left in such storage areas are left at their owner's risk. It is recommended that if personal mobile devices are stored, they should be security marked, password protected and insured. No liability for loss and/or damage can be accepted by the provision.

Emergency contact

Mobile devices 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 devices should therefore be promoted. This affords practitioners and managers peace of mind, by reducing stress and worry and therefore allows them to concentrate more fully on their work. Such use must be subject to management, monitoring and review.

Exemplar Misuse of Information and Communication Technology Policy

This exemplar policy is intended to be used as a template for a wide range of provisions and should be amended to meet the needs of each provision.

Introduction

Technology is part of everyday life and should be embraced as it can facilitate learning and development for both practitioners and children. However, it is important to recognise the associated risks and to minimise these by promoting the positive and responsible use of technology among staff and children. Practical steps should also be taken to ensure that there are mechanisms in place to deal with any misuse.

Aim

The Misuse of Information and Communication Technology Policy aims to ensure that any allegation, which is made in respect of the intentional or unintentional misuse of any online technologies, is addressed in a responsible and calm manner. This includes any known or suspected breaches of the provision's acceptable use agreements (AUA), Digital and Video Images Policy, Internet Policy and Mobile Devices Policy.

Allegations must be dealt with promptly, sensitively and fairly in line with agreed procedures. The Misuse of Information and Communication Technology Policy should also outline the strategies employed in response to misuse that are applied if an incident occurs.

The overall priority should be to ensure the safety and well-being of children at all times. If it is suspected at any stage that a child may have been or is considered to be subject to abuse, the provision's Safeguarding Policy and procedures should be implemented with immediate effect. These procedures should also be followed if an allegation of abuse is made against any employee, manager, volunteer or student. The Safeguarding Policy should take precedence over all others, and referrals should be made to the appropriate agency as deemed necessary.

Scope

The Misuse of Information and Communication Technology Policy applies to all individuals who have access to and/or are users of work-related systems. This includes children, parents/carers, practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

The policy should be implemented in respect of any potential breaches of the provision's AUA, Digital and Video Images Policy, Internet Policy and Mobile Devices Policy.

Responsibilities

The person responsible for safeguarding/child protection is responsible for ensuring that the procedures outlined in this policy are followed. These procedures should be followed if an allegation of misuse is made against a child or an adult.

(Further details on responsibilities can be found in the 'Acceptable use agreements' section of this guidance (see page 13).)

Policy statement

Clear and well-publicised policies and procedures which will influence practice are the simplest and most effective way for the safe use of technology to be upheld. Such policies and procedures should ensure the promotion of acceptable use and clearly define those behaviours which are not. The strategies employed in response to misuse and responsible use should be identified.

It is important that:

- relevant online safety policies and procedures are fully implemented, monitored and reviewed, and these policies and procedures should be rigorous, manageable and reflective of practice, and shared with all users in the provision environment – the person responsible for safeguarding/child protection is responsible for the management of such policies
- all users in the provision environment should be made aware of possible signs of potential misuse – adults, in particular, are responsible for observing practice and behaviours, so that any significant changes in such are identified at the earliest opportunity
- all users in the provision environment should be made aware that the misuse of technology and/or breaches of relevant policies and procedures are taken seriously, and that strategies employed in response to misuse and responsible use are clearly defined and could be applied, should concerns be raised
- effective reporting and whistleblowing procedures are in place and promoted.

It should be acknowledged, however, that no system or procedure can be considered completely safe, secure and foolproof. It should, therefore, be accepted that the potential for technology to be misused, whether intentionally or unintentionally, will remain. The aim of the Misuse of Information and Communication Technology Policy is therefore to minimise such opportunities and risk.

Procedures

General

All incidents should be dealt with on an individual case-by-case basis, and an escalating tariff of agreed strategies employed in response to misuse should be put in place.

The context, intention and impact of each incident should determine the response and actions to be taken. This allows a degree of flexibility in the application of strategies employed in response to an incident. For example, a series of minor incidents by one individual is likely to be treated differently than a one-off occurrence. Similarly, unintentional and intentional access to inappropriate websites will instigate different

levels of intervention and response (see supporting document 11 (Guidance for reviewing internet sites (for suspected incidents of harassment/distress)) and supporting document 12 (Record of reviewing internet sites (for suspected incidents of harassment/distress)) of the toolkit[33]).

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

All incidents

The following procedure should be followed for all incidents.

- The incident should be reported to the person responsible for safeguarding/child protection. A written incident record should be made, and the situation monitored.
- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident may be escalated to a 'serious' level.
- If the incident relates to the inadvertent access to an inappropriate website, this should be added to the banned or restricted list and filters should be applied, where relevant.
- In respect of misuse by children, parents/carers must be informed of the alleged incident and should be advised of any actions to be taken as a result.
- Strategies for managing misuse should be applied in accordance with the AUA.

There will always be the possibility that through access to the internet children may gain unintentional access to inappropriate materials. Such content may not be deemed offensive in a different context, or illegal in nature, but is unsuitable in a childcare environment and should be acted upon.

Reporting

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

Serious incidents

All serious incidents must be dealt with promptly and reported to the person responsbile for safeguarding/child protection immediately.

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

Appropriate actions should be agreed between the person responsible for safeguarding/child protection and the relevant senior manager. All details should be accurately and legibly recorded. The reason why any decision is made should also be noted.

---

[33] hwb.gov.wales/repository/resource/397d9856-5d5d-42e8-b81f-7dca790b7243/en

If at any stage a child is or has been subject to abuse of any form, the provision's Safeguarding Policy should be implemented with immediate effect. A referral should be made through relevant local safeguarding/child protection procedures or through children's social care and the police, where applicable.

If the incident relates to an allegation made against an employee, manager, volunteer or student, and there is a suggestion that a child has been subject to any form of abuse, the provision's Safeguarding Policy will again be implemented with immediate effect. The local authority must be contacted in the first instance in respect of any allegation made against an adult. The police and the Care Inspectorate Wales (CIW) (where relevant) must also be contacted.

No internal investigation or interviews should be carried out in respect of any allegations, unless explicitly requested otherwise by an investigating agency.

If allegations of abuse are made, children's social care, the police and/or the local authority will be the investigative bodies. It must therefore be ensured that no action is taken which could compromise any such investigations.

Where applicable, any device or hardware implicated in any potential investigations of misuse should be secured, so that evidence can be preserved. This may include mobile devices, laptops, computers and portable media technology.

Internal disciplinary procedures should not be undertaken until investigations by the relevant agencies 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.

On completion of both internal and external investigations, or sooner where appropriate, an online safety review should be undertaken and relevant policies and procedures amended and updated as necessary. A consultation on any proposed revisions should be held with all users in the provision environment as appropriate. Revised policies and procedures should be circulated as applicable.

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

The following incidents must always be reported to the police, and (where relevant) contact must be made with child protection services, children's social care, the local authority, the police and Care Inspectorate Wales (CIW):

- discovery of indecent images or videos of children and young people
- behaviour considered to be 'grooming'
- sending of obscene materials
- attempts to radicalise or the sharing of extremist views.

By not reporting such incidents, an offence may be committed.

No attempt should be made to download, print or send any materials found. Further offences could be committed by doing so.

If potentially illegal material is discovered, as far as is reasonably practical, the equipment or materials found should not be touched. Content should not be deleted or forwarded. Secure the device and retain password/access rights until passed to the police. Devices should not be switched off unless 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.

A report should also be made to the Internet Watch Foundation[34] in the event that potentially illegal image(s) or video(s) of child sexual abuse have been accessed online, giving details of the website address. If it is unclear whether the content is illegal or not, the concern should be reported as a matter of caution.

Media attention

If a serious incident occurs, it may attract intense media interest and speculation. On such occasions, every possible attempt should be made to ensure that children, staff and parents/carers are protected and supported appropriately.

An agreed media strategy should be implemented and statements only released by authorised personnel, in accordance with information-sharing procedures. In all instances, the prime concern should be the safeguarding and welfare of the children and their families. Seek advice before any media engagement is undertaken.

[34] www.iwf.org.uk

Useful information, resources and contacts

Useful information, resources and contacts

Care Inspectorate Wales (CIW)

Care Inspectorate Wales (CIW) inspect and take action to improve the quality and safety of services for the well-being of the people of Wales. This includes all early years provision in non-maintained settings in Wales such as childminders and children's daycare services.

https://careinspectorate.wales

Child Exploitation and Online Protection (CEOP)

Resources for children, parents/carers and practitioners from the Child Exploitation and Online Protection Centre.

www.thinkuknow.co.uk

Estyn

Estyn is the office of Her Majesty's Inspectorate for Education and Training in Wales. It is independent of, but funded by, the Welsh Parliament, and its purpose is to inspect quality and standards in education and training in Wales.

www.estyn.gov.wales

Online Compass self-review tool

For a provision based in a school, 360 degree safe Cymru[35], developed by South West Grid for Learning (SWGfL) on behalf of the Welsh Government, is a powerful self-review tool for reviewing online safety procedures.

The Online Compass self-review tool is relevant to other provisions and has been written for smaller organisations. The self-review tool will not only audit current provision, but will also benchmark progress, provide clear advice on how to progress further, manage reports, and help develop and identify future planning and training needs.

www.onlinecompass.org.uk

[35] To access 360 degree safe Cymru on Hwb, users in provisions/schools should log in to Hwb and click on the link to the 360 tool under Hwb tools.

Online safety helpline for professionals

The UK Safer Internet Centre has been funded by the European Commission to provide a helpline for professionals who work with children and young people in the UK, specifically tackling the area of online safety.

The helpline provides support with all aspects of digital and online issues such as social networking sites, online bullying, sexting, online gaming and safeguarding/child protection online. It aims to resolve issues that professionals face about themselves, such as protecting professional identity and reputation, as well as young people in relation to online safety.

Telephone: 0344 381 4772* Monday to Friday, 10am to 4pm

The helpline can be called at any time, and calls will be responded to during their normal working hours.

* *Calls cost the same as standard landline numbers that start with '01' or '02'. If your phone tariff offers inclusive calls to landlines, calls to 0344/5 numbers will also be included in the same way.*

Online Safety Live

Free online safety events delivered across the whole of the UK by South West Grid for Learning (SWGfL) on behalf of the UK Safer Internet Centre. Events are local and include all the very latest in online safety including the latest issues, biggest trends and best resources.

The events are two hours long and cover a broad range of online safety topics, and at the end of the event all delegates receive access to an online resource area containing links to all the materials mentioned, signposting to sources of help and support as well as a live copy of the presentation itself.

www.saferinternet.org.uk/training-events/online-safety-live-free-online-safety-events

'Keeping safe online' area on Hwb

This area offers a wealth of resources for learners, schools and parents/carers on a wide range of online safety topics. The information has been carefully crafted to reflect current trends and thinking around online safety topics.

hwb.gov.wales/keepingsafeonline

South West Grid for Learning (SWGfL)

South West Grid for Learning (SWGfL) is a not-for-profit charitable trust providing resources and services to improve the use of technology by young people. The website provides continuously updated information and resources for all areas of technology and online safety for young people.

https://swgfl.org.uk

UK Council for Internet Safety (UKCIS)

The UK Council for Internet Safety (UKCIS) is a collaborative forum through which government, the tech community and the third sector work together to ensure the UK is the safest place in the world to be online.

www.gov.uk/government/organisations/uk-council-for-internet-safety

UK Safer Internet Centre

The UK Safer Internet Centre provides information on how to use the internet and new technologies safely and responsibly. There is also a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies.

www.saferinternet.org.uk

Welsh Government

The Welsh Government has relevant Foundation Phase information available, including the *Foundation Phase Framework* and guides for parents/carers.

https://gov.wales/foundation-phase-framework

Additional websites for parents/carers

The following websites are aimed at parents/carers and provide tips for keeping young children safe online. This includes information on age-appropriate social networks, apps and games.

www.childnet.com/resources/keeping-under-fives-safe-online

www.commonsensemedia.org/reviews

www.net-aware.org.uk

www.saferinternet.org.uk/advice-and-resources/parents-and-carers

www.internetmatters.org/advice/0-5