Whitegate Nursery School

Working together to make a real and lasting difference...

Online Safety/Acceptable Use Policy

This policy outlines our purpose in providing access to the Internet at Whitegate Nursery School explains how the School is seeking to avoid the potential problems that unrestricted Internet access could give rise to. This policy has been updated in line with the Lancashire 'Primary E-Safety' Guidance and 'Online Safety – A Toolkit for Early Years Settings' recommendations. The policy covers internet use by children, families and staff.

Our Mission Statement

Our Nursery School strives to provide a happy, caring and understanding environment, where each individual is valued and is able to develop to their full potential within the Early Years Foundation Stage

We aim to provide an integrated service which involves and supports parents in the care and education of their children. For very young children, care and education are inseparable.

Aims

- To safeguard children by promoting appropriate and acceptable use of ICT.
- To outline the roles and responsibilities of all individuals who have access to work related ICT
- To ensure children, families and staff who use ICT are aware of the risk and have a clear understanding of what constitutes misuse and the sanctions that may be applied
- To outline safe and effective practice in the use of the internet. It provides advice on acceptable use and effective measures to enable children, families and staff to use ICT resources in a safer online environment.
-

Rationale

Children are using technology in ever increasing ways to enhance and enrich their learning and lifestyles. Children actively seek new and imaginative ways to communicate and develop their skills. It is the responsibility of the school to provide children with a safe environment in which to explore technology and the internet. The school will ensure that e-safety is a priority.

Internet access in the school

We are providing ICT, Internet access and Email access for staff in order to:

- support and extend skills and knowledge across the areas of learning
- motivate all children, enhance interactive learning and have fun
- support all children including those with Special Education Needs and the Able Gifted and Talented
- to equip children and staff with a life skill which is essential for future education and the world of work
- support the professional work of staff
- enhance the school's management information and business administration systems
- to improve methods of communication between schools, the LA, DfES, parents and other partners
- to improve the ICT skills of users of the Nursery School through courses

Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff and any other adults involved in supervising children accessing the internet, will have access to the School's Internet Safety Policy, and will have its importance explained to them and will sign and Staff Acceptable Use agreement *(see appendix 1)
Parents' attention will be drawn to the Policy by signing a Parents Acceptable Use agreement. Our school AUP/Internet Safety Policy will be available for parents and others to read both in school and on our website (www.whitegate.org)

The educational benefits of using ICT, the Internet and Email include:

- Access to world-wide educational resources and information including pictures, games, music and applications (apps).
- communication with advisory and support services, professional associations and colleagues
- providing a means of communication between staff & pupils, parents & others in the community
- obtaining a range of technical support
- encouraging electronic literacy
- the development of fine motor skills

ICT and the Internet can provide an effective medium for learning where:

- internet access is planned to enrich and extend learning activities as an integrated aspect of the curriculum
- children are given a clear purpose for Internet use
- children are provided with relevant and suitable Websites and applications (apps)
- children are monitored in their use of the Internet
- the whole staff have been given opportunities to discuss the issues around developing good teaching strategies

Using the internet to enhance learning

In the Nursery School Internet access is regarded as a necessary part of the statutory curriculum and access to the Internet will only be authorised on the basis of educational need.

- Pupils will be provided with suitable web based activities/apps
- Access to the Internet will become a planned part of the daily EYFS curriculum
- Pupils accessing the Internet will be supervised by an adult at all times.

Target Tracker

Target Tracker is a programme created and managed by Juniper Education© which is used as an assessment and record of learning tool by staff at Whitegate. This programme is accessible via ipad and desktop PC via username and password which is individual to each user. User rights vary and are controlled by the Headteacher. Juniper Education© Privacy Policy (see Appendix 6) ensures all data collected via the Target Tracker program including photographs and personal data about children will be kept secure.

CPOMS

Cpoms is a record system we use alongside our safeguarding policies and procedures to record any safeguarding and welfare concerns or information. This information is kept in a secure cloud evidenced by CPOMS privacy policy. This information is kept secure and only shared with schools as the children move from Nursery into School. Each member of staff has an individual login and information they input will be shared with DSL and Deputy DSL's only. The DSL and Deputy DSL have a higher level of access which enables them to see all information inputted into the system and can amend any information as necessary.

Risks associated with using ICT

The risks associated with using ICT can be categorised into four areas:

Content

In common with other media such as magazines, books and videos and social media sites, some material available via the Internet is unsuitable. The School will take all reasonable precautions to ensure that such material is inaccessible, through LA filtering systems and supervision. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a terminal. However neither the School or the LA can accept liability for the material accessed, or any consequences thereof.

Contact

E-safety risks associated with contact receive the most press attention because of the fear of physical danger. A criminal minority makes use of the internet and related services, chat rooms, gaming and social media software, to make contact with others. The intention of these people is to establish and develop inappropriate relationships. There is also a risk that while online, people might provide information that can identify them or others; or arrange to meet people they have met online, thus posing a risk to their safety or that of family and friends. New technologies provide an apparently anonymous method by which bullies can target victims at any time, via e-mail, online chat and social sites. This can damage self-esteem and pose a psychological threat. These technologies can also enable identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords.

Conduct

As e-commerce continues to grow, privacy issues arise and there is a risk that people may give out personal information of family or friends with unexpected consequences. Junk e-mail or spam can appear realistic, people may be tricked into revealing personal or financial information that could be used for identity theft or premium rate services on mobile phones, ipads or on apps. Children may not

differentiate between what is advertising and what is not. All people involved with children must consider their digital footprint and online reputation and how this may affect their lives and the lives of those around them. As a school we will work to ensure staff, parents and children conduct themselves appropriately when using the internet or internet based programmes.

Culture

Cultural e-safety risks cut across the other three areas. Safety messages should be frequently reinforced to become embedded. There is a risk that individuals may get involved in inappropriate or anti-social behaviour while using new technologies. People can easily access adult social networking sites, publishing, collaborating and sharing information of an adult nature. Plagiarism and copyright are also key cultural issues, copying work or downloading music, games or apps.

Responsibilities of the School:

- staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken to protect children
- the Head Teach and ICT Champion will ensure that the policy is implemented effectively
- policy and procedures will be reviewed as Internet use expands
- we will ensure that occasional checks are made on files to monitor compliance with the School's Policy and staff will be informed that such checks are made
- the school will ensure that children are always supervised when using the Internet
- all machines with Internet capability are accommodated in public areas and their use is frequently monitored
- the school will only use an Internet service provider with a proxy server to filter the material available or will take measures to ensure similar protection is installed on the school's computer system
- the school will do its utmost to ensure that children cannot disable the proxy server or interfere with protection software
- the school will ensure that virus protection is installed and updated regularly
- any material that the school suspects is illegal/inappropriate will be reported to the designated DSP by filling in a reporting log (see appendix 2 & 3)
- the school will ensure systems to protect children are reviewed and improved regularly
- Staff logon details are created by the office administrator and staff are required to create a password that is then kept private
- staff will log onto the server using the staff username and password and log off after use

- Administrator passwords are kept in a secure location and use by designated members of staff
- Staff members in the school will support and work with families to understand e-safety, including the risks posed by online activity, extremist views and radicalisation.

Responsibilities of staff and children:

- Children will only access the internet though the pupil logon created by the school, which will limit their access to curricular sites, games and applications only
- if staff, children or parents discover unsuitable sites, the URL (address) and content will be reported to the DSL who will then log this with BT Lancashire Services
- children using the Internet will be supervised appropriately
- staff should obtain permission before downloading software or apps from the Internet, checking copyrights
- staff should not use the Internet for personal use unless with the permission of their line manager and this may be given in exceptional circumstances (see Staff Code of Conduct)
- staff may loan a school laptop. An in house loan agreement must be completed and complied with.
- Teaching staff will have the use of a school iPad to use as a tool to supporting teaching and learning. The in house loan agreement and AUP must be completed and complied with.
- Staff will strive to promote Staying Safe Online (http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/) and safe internet use when working with children. This will cover a wide range of safety messages including developmentally appropriate messages related to the Prevent Agenda (see appendix 4)

Additional guidance for staff

Staff should:

- keep all logins and passwords strictly private and always log off correctly after using any computer in school, including laptops and ipads
- report immediately any inappropriate or malicious web pages accessed or emails received to the Head Teacher
- be aware that the access of any inappropriate or malicious material can result in criminal proceedings
- be aware that accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and,

if proven, will invariably lead to the individual being barred from work with children and young people (see Staff Code of Conduct)

- if using a laptop or iPad, ensure it is properly password protected, to protect personal data stored
- ensure that children's personal information (reports, curriculum development records) and photographs are not stored on personal home computers or laptops after official use
- if a personal or school laptop is used at home, ensure different users are set up in Windows
- iPads are not used for unofficial use at home or at work and must be locked away after use (A home loan agreement is in place to support access to iPads for work related use at home)
- ensure any software installed on computers or laptops, in school and at home, is covered by the school license agreement
- check copyrights of pictures, music, websites and apps downloaded
- never use personal email, mobile phones and websites, (such as MSN Messenger or Facebook) to contact parents or children.
- The school has its own Facebook account and text messaging service to support communication with parents.
- staff should not give their personal details such as home or mobile telephone number, home e-mail address to children or parents
- staff should use mobile telephones when working in the community or taking children on excursions; these phones should have no camera facility
- staff will not use the 's Wi-Fi connection on their personal mobiles at any time
- if electronic information regarding the School is to be taken away from the school by a member of staff at any time this must be carried on an encrypted and secure USB stick provided or approved by the Head Teacher.
- When on school business off the premises, personal mobile phones must not be used and should remain on school premises. A School mobile will be provided for business use.

The use of social networking sites and other forms of social media

Employees who choose to make use of social networking sites/media should:

- familiarise themselves with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended.
- Do not conduct or portray themselves in a manner which may:
    - Bring the school into disrepute.
    - Lead to valid parental complaints.
    - Be deemed as derogatory towards the school and/or its employees
    - Be deemed as derogatory towards pupils and/or parents and carers.
    - Bring into question their appropriateness to work with children and young people.

Do not form on-line ‘friendships’ enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to the Specific Guidance points above.)

All employees should be aware that disciplinary action maybe taken if they choose not to follow the guidance outlined.

The management of e-mail in the School:

- email is regarded as an essential means of communication and the school will take appropriate steps to monitor its use and content communication using e-mail will be organised to ensure it is for appropriate business and educational use and not for private or personal messages
- the language and content of e-mails should be of an appropriate level expected of any written work and should ensure that the good name of the School is maintained
- the forwarding of chain letters and anonymous letters is banned
- staff should be aware that all e-mail on the School system is regarded as public and as such will be monitored and may be printed out an posted on public notice boards
- staff will be informed how to deal with unacceptable material such as chain letters, hoaxes, virus infections or offensive material

- e-mail messages on School and business (e.g. arranging a visit) must be approved by a line manager before sending and should be regarded as having been sent on headed notepaper
- e-mail and the Internet should not be used to order materials or undertake any activity which incurs a cost to the school without the Head Teachers prior consent.
- staff should be made aware of the potential for virus infection through the sending of files attached to e-mails
- personal use is not permitted unless in exceptional circumstances and with the permission of a line manager
- the use of social networking sites to discuss work related events and colleagues is contrary to the School 's Code of Conduct and will be dealt with as per disciplinary procedures (The School has its own Facebook account to support communication with families)
- use of equipment for personal use is contrary to the Code of Conduct
- access to newsgroups and chat rooms is not seen as appropriate use
- e-mail messages will be filtered for content in a managed system
- all outgoing messages from the will have a tag line or signature giving details of the and who to contact if the message is offensive
- virus protection is kept up to date and all e-mails are checked for viruses

Our School/ e-mail system must not be used for:

- the distribution or forwarding of material which could be taken to be offensive by anyone reading the message
- sending material which contains any abusive or offensive language
- sending messages which may be threatening or bullying in nature
- sending personal details to a third party
- sending private information about another individual to a third party without permission
- any activities which involve personal financial transactions
- forwarding chain letters
- forwarding large graphics
- sending viruses or hoax messages
- sending attachments unless specifically agreed in the policy
- participating in newsgroups and chat rooms

Publishing material on the website:

- the School will maintain editorial responsibility for any initiated web site to ensure that content is accurate and quality of presentation is maintained
- the web site will comply with the School's guidelines for publications
- all material must be the author's own work, credit should be given, it must state clearly the author's identity or status and not break copyright
- the point of contact on the web site will be the School's address, e-mail and telephone number. Home information or individuals' e-mail addresses will not be published

- photographs of identifiable individual children will not be published on the web site without the consent of parents. Group photographs should not have a name list attached. Identities of children must be protected at all times
- parental consent will be sought before publishing photographs of children

Communicating to stakeholders via ICT

Parent App

Parent App is a communication tool which is used to communicate and share information with the school's stakeholders. Parent App will be used to:

- Share important information such as term dates and school closures
- Send learning resources to parents to support home learning
- Allow parents to communicate absences
- Share policies and procedures
- Access links to the school's social media such as Facebook, Instagram and our website
- Send messages to specific stakeholders

For how Parent App keep our data secure please visit **https://www.parentapps.co.uk/privacy-policy**

Facebook, Twitter and Instagram

The Nursery School will use these social media sites to promote and share learning and key information with stakeholders. Media will be chosen in accordance to the permissions list compiled from children's personal data forms completed by parents on entry. Data will be protected by each social media sites privacy policy (see Appendix for individual media sites privacy policies)

Maintaining the security of the School's ICT network:

We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.
The ICT technician will up-date virus protection regularly. The Head Teacher, Leadership Team and ICT Champion will keep up-to-date with ICT news; developments and work with the LA and Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

Lightspeed Filtering Systems

At Whitegate we use the Lancashire internet filtering solution to ensure children's, staff and other adults who use our networks safety whilst using the internet. Lightspeed is an internet filtering solution provided by BT Education

Services for Lancashire Schools. This helps to ensure all content accessible through our network is deemed appropriate for all users. This filtering solution is controlled by BT Lancashire Schools and removes/blocks any context which may be deemed inappropriate. Staff are able to log a call immediately with BTLS if they believe a website or piece of content is deemed inappropriate, also they can check a website they may want to use as a learning tool to check it is suitable by entering the URL into https://archive.lightspeedsystems.com/, where it will checked against Lancashire's filtering systems and identified as appropriate or inappropriate.

Lightspeed Systems also work to support the Prevent Duty (see Appendix 5)

Procedure for dealing with complaints and breaches of conduct:

- any complaints or breaches of conduct will be dealt with promptly
- responsibility for handling incidents will be given to the School Leadership Team, recorded and reported to the Head Teacher
- the facts of the case will need to be established,
- there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

Informing staff, children and parents:

- all staff will be involved in developing and reviewing the Internet Safety policy
- parents' attention will be drawn to the Policy (accessible on the School Website)
- demonstrations and practical ICT courses for parents are organised throughout the year and support parental awareness, knowledge and skills in relation to ICT
- Internet safety will form a part of the ICT courses held regularly at the School
- The reception area is a mobile friendly zone for parents. Use of mobile devices is not permitted in any other area of the building. For parents who visit the School we can keep mobiles securely in the safe or locked cabinet.

Internet access and parent partnerships

Parents will be informed in initial visits to the School that children are provided with supervised Internet access as part of their curriculum. We will keep parents in touch with future ICT developments by letter and newsletter.
Internet use in children's homes is rapidly increasing and some parents may be grateful for any advice/guidance that the School can offer – especially with regard to safe access for children. The School is willing to offer advice and suggest alternative sources of advice on the understanding that neither the School or the LA can be held responsible for the consequences of such advice.

APPENDIX

This policy draws on the following references:

Lancashire 'Primary E-Safety' Guidance and 'Online Safety' – A Toolkit for Early Years Settings http://www.lancsngfl.ac.uk/esafety/

Kent NGfL Website
Latest version of the Kent policy www.kent.gov.uk/ngfl/policy.html

ITCAS Web site www.kirklees-ednet.org.uk/itcas/support
Discussion document on use of Internet
Guidance to protect staff using electronic communications

Connecting Schools: Networking People
www.ngfl.gov.uk/reference/publications/connecting

DfEE / BECTa April 1998 Tel. 0845 6022260 (free order line)

Preventing the Misuse of Computers in Schools
British Computer Society www.bcs.org.uk/news/misuse.htm

Association for Co-ordinators and Teachers of IT (ACITT)
Acceptable Use Policy for UK Schools www.acitt.org.uk/aup.html

Parents' Information Network (PIN)
Leaflets www.pinlift.org.uk

NCH Action for Children
A Parents' Guide www.nchafc.org.uk

Home Computers and Children
www.becta.org.uk/projects/censor

BECTa leaflet Tel: 01203 416994

Censorship Issues
BECTa www.becta.org.uk/projects/censor/

Internet Watch Foundation www.iwf.org.uk

Reporting illegal Internet material Tel: 0845 600 8844

NAACE/British Computer Society www.bcs.org.uk/iap.html

Safety Net Kids: Staying Safe Online:
http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/

The Prevent Duty –
Protecting Children from radicalisation: departmental Advice for Schools and Childcare providers **https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty**

Facebook Privacy Policy - https://www.facebook.com/policy.php

Twitter Privacy Policy - https://twitter.com/en/privacy

Instagram Privacy Policy - https://help.instagram.com/519522125107875

CPOMS Privacy Policy https://www.cpoms.co.uk/privacy-statement/

Additional Documents

Appendix 1

Whitegate Nursery School
Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of the Headteacher.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have been given a copy of the Acceptable Use Policy and have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……..……..……

Date …….……..……..

Full
Name……..……..…(PRINT)

Position/Role
……

When you have read the attached policy and have signed please hand the slip to the office.

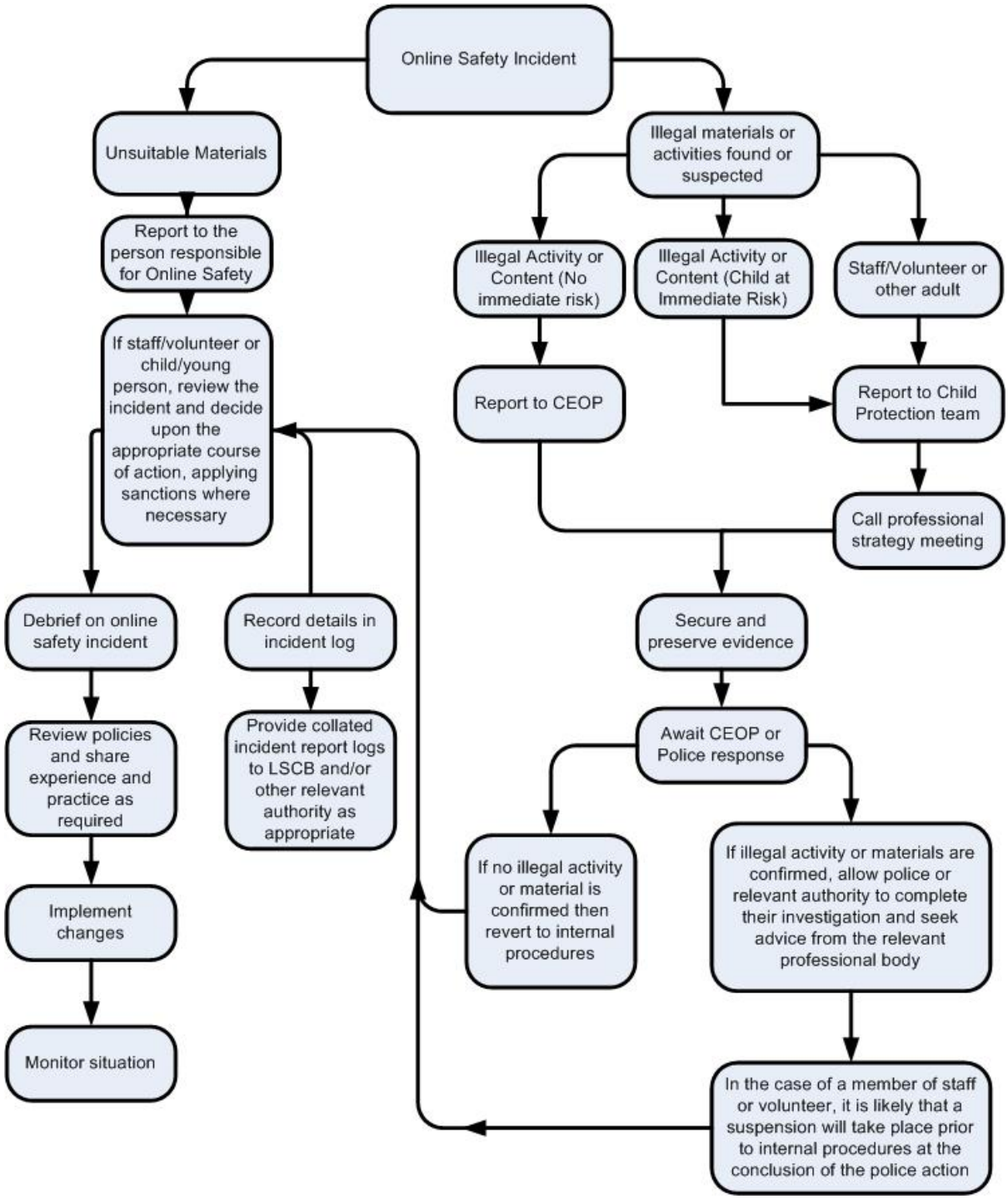
Appendix 2 – Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 3 – Responding to incidents of misuse flow chart



Appendix 4

The Prevent duty

Departmental advice for schools and childcare providers

June 2015 2

Contents

Summary

About this departmental advice

This is departmental advice from the Department for Education. This advice is non-statutory, and has been produced to help recipients understand the implications of the Prevent duty. The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Expiry or review date

This advice will next be reviewed before September 2016.

Who is this advice for?

This advice is for:

• Governing bodies, school leaders and school staff in maintained schools (including nursery schools), non-maintained special schools, proprietors of independent schools (including academies and free schools), alternative provision academies and 16-19 academies

• Management committees and staff in pupil referral units

• Proprietors and managers and staff in registered childcare settings

It will be of particular interest to safeguarding leads.

Main points

The main points of this advice are to:

• explain what the Prevent duty means for schools and childcare providers;

• make clear what schools and childcare providers should do to demonstrate compliance with the duty; and

• inform schools and childcare providers about other sources of information, advice and support.

Introduction

From 1 July 2015 all schools must have regard to the statutory guidance. Paragraphs 57-76 of the guidance are concerned specifically with schools and childcare providers. [1], registered early years childcare providers[2] and registered later years childcare providers[3] (referred to in this advice as 'childcare providers') are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. It applies to a wide range of public-facing bodies. Bodies to which the duty applies

[1] Including early years and later years childcare provision in schools that is exempt from registration under the Childcare Act 2006.
[2] Those registered under Chapter 2 or 2A of Part 3 of the Childcare Act 2006, including childminders.
[3] Those registered under Chapter 3 or 3A of Part 3 of the Childcare Act 2006, including childminders.
[4] "Radicalisation" refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism. During that process it is possible to intervene to prevent vulnerable people being drawn into terrorist-related activity.

This advice complements the statutory guidance and refers to other relevant guidance and advice. It is intended to help schools and childcare providers think about what they can do to protect children from the risk of radicalisation[4] and suggests how they can access support to do this. It reflects actions that many schools and childcare providers will already be taking to protect children from this risk.

The Prevent duty: what it means for schools and childcare providers

In order for schools and childcare providers to fulfil the Prevent duty, it is essential that staff are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified. Protecting children from the risk of radicalisation should be seen as part of schools' and childcare providers' wider safeguarding duties, and is similar in nature to protecting children from other harms (e.g. drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences.

Schools and childcare providers can also build pupils' resilience to radicalisation by promoting fundamental British values and enabling them to challenge extremist[5] views. It is important to emphasise that the Prevent duty is not intended to stop pupils debating controversial issues. On the contrary, schools should provide a safe space in which children, young people and staff can understand the risks associated with terrorism and develop the knowledge and skills to be able to challenge extremist arguments. For early years childcare providers, the statutory framework for the Early Years Foundation Stage sets standards for learning, development and care for children from 0-5, thereby assisting their personal, social and emotional development and understanding of the world.

[5] "Extremism" is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas. Terrorist groups very often draw on extremist ideas developed by extremist organisations.

The Prevent duty is entirely consistent with schools' and childcare providers' existing responsibilities and should not be burdensome. Ofsted's revised common inspection framework for education, skills and early years, which comes into effect from 1 September 2015, makes specific reference to the need to have safeguarding arrangements to promote pupils' welfare and prevent radicalisation and extremism. The associated handbooks for inspectors set out the expectations for different settings. The common inspection framework and handbooks are available on GOV.UK.

The statutory guidance on the Prevent duty summarises the requirements on schools and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies. This advice focuses on those four themes.

Risk assessment

The statutory guidance makes clear that schools and childcare providers are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This means being able to demonstrate both a general understanding of the risks affecting children and young people in the area and a 6

specific understanding of how to identify individual children who may be at risk of radicalisation and what to do to support them.
The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context. It is important that schools and childcare providers understand these risks so that they can respond in an appropriate and proportionate way. At the same time schools and childcare providers should be aware of the increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet. The local authority and local police will be able to provide contextual information to help schools and childcare providers understand the risks in their areas.
There is no single way of identifying an individual who is likely to be susceptible to a terrorist ideology. As with managing other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Children at risk of radicalisation may display different signs or seek to hide their views. School staff should use their professional judgement in identifying children who might be at risk of radicalisation and act proportionately. Even very young children may be vulnerable to radicalisation by others, whether in the family or outside, and display concerning behaviour. The Prevent duty does not require teachers or childcare providers to carry out unnecessary intrusion into family life but as with any other safeguarding risk, they must take action when they observe behaviour of concern.
Schools and childcare providers should have clear procedures in place for protecting children at risk of radicalisation. These procedures may be set out in existing safeguarding policies. It is not necessary for schools and childcare settings to have distinct policies on implementing the Prevent duty. General safeguarding principles apply to keeping children safe from the risk of radicalisation as set out in the relevant statutory guidance, Working together to safeguard children and Keeping children safe in education.
School staff and childcare providers should understand when it is appropriate to make a referral to the Channel programme. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual's engagement with the programme is entirely voluntary at all stages. Detailed guidance on Channel is available.
An online general awareness training module on Channel is available. The module is suitable for school staff and other front-line workers. It provides an introduction to the topics covered by this advice, including how to identify factors that can make people vulnerable to radicalisation, and case studies illustrating the types of intervention that may be appropriate, in addition to Channel.

Working in partnership

The Prevent duty builds on existing local partnership arrangements. Local Safeguarding Children Boards (LSCBs) are responsible for co-ordinating what is done by local agencies for the purposes of safeguarding and promoting the welfare of children in their local area. Safeguarding arrangements should already take into account the policies and procedures of the LSCB. For example, LSCBs publish threshold guidance indicating when a child or young person might be referred for support.

Local authorities are vital to all aspects of Prevent work. In some priority local authority areas, Home Office fund dedicated Prevent co-ordinators to work with communities and organisations, including schools. Other partners, in particular the police and also civil society organisations, may be able to provide advice and support to schools on implementing the duty.

Effective engagement with parents / the family is also important as they are in a key position to spot signs of radicalisation. It is important to assist and advise families who raise concerns and be able to point them to the right support mechanisms.

Staff training

The statutory guidance refers to the importance of Prevent awareness training to equip staff to identify children at risk of being drawn into terrorism and to challenge extremist ideas. The Home Office has developed a core training product for this purpose – Workshop to Raise Awareness of Prevent (WRAP). There are a number of professionals – particularly in safeguarding roles - working within Local Authorities, the Police, Health and Higher and Further Education who are accredited WRAP trained facilitators. We are working to build capacity within the system to deliver training.

Individual schools and childcare providers are best placed to assess their training needs in the light of their assessment of the risk. As a minimum, however, schools should ensure that the Designated Safeguarding Lead undertakes Prevent awareness training and is able to provide advice and support to other members of staff on protecting children from the risk of radicalisation. We recognise that it can be more difficult for many childcare providers, such as childminders, to attend training and we are considering other ways in which they can increase their awareness and be able to demonstrate that. This advice is one way of raising childcare providers' awareness. 8

ICT policies

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet website.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

Building children's resilience to radicalisation

As explained above, schools can build pupils' resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Schools are already expected to promote the spiritual, moral, social and cultural development of pupils and, within this, fundamental British values. Advice on promoting fundamental British values in schools is available.

Personal, Social and Health Education (PSHE) can be an effective way of providing pupils with time to explore sensitive or controversial issues, and equipping them with the knowledge and skills to understand and manage difficult situations. The subject can be used to teach pupils to recognise and manage risk, make safer choices, and recognise when pressure from others threatens their personal safety and wellbeing. They can also develop effective ways of resisting pressures, including knowing when, where and how to get help. Schools can encourage pupils to develop positive character traits through PSHE, such as resilience, determination, self-esteem, and confidence.

Citizenship helps to provide pupils with the knowledge, skills and understanding to prepare them to play a full and active part in society. It should equip pupils to explore political and social issues critically, to weigh evidence, to debate, and to make reasoned arguments. In Citizenship, pupils learn about democracy, government and how laws are made and upheld. Pupils are also taught about the diverse national, regional, religious and ethnic identities in the United Kingdom and the need for mutual respect and understanding. A number of resources are available to support schools in this work. These include products aimed at giving teachers the confidence to manage debates about contentious issues and to help them develop their pupils' critical thinking skills. Local authorities and the local police may be able to advise on the resources which are available. In some cases these resources may be charged for, particularly where they are 9 . 10

What to do if you have a concern

As explained above, if a member of staff in a school has a concern about a particular pupil they should follow the school's normal safeguarding procedures, including discussing with the school's designated safeguarding lead, and where deemed necessary, with children's social care. In Prevent priority areas, the local authority will have a Prevent lead who can also provide support.

You can also contact your local police force or dial 101 (the non-emergency number). They can talk to you in confidence about your concerns and help you gain access to support and advice.

The Department for Education has dedicated a telephone helpline (020 7340 7264) to enable staff and governors to raise concerns relating to extremism directly. Concerns can also be raised by email to counter.extremism@education.gsi.gov.uk. Please note that the helpline is not intended for use in emergency situations, such as a child being at immediate risk of harm or a security incident, in which case the normal emergency procedures should be followed. 11

Appendix 5

From the Lightspeed Systems website:

http://www.lightspeedsystems.com/en-uk/prevent-duty/

Safeguarding Tools

Lightspeed Systems Web Filter contains billions of URL's all arranged into education-focused categories. Most categories can be allowed or blocked by admins to ensure schools have granular control over the content students can see. However, there are a number of sealed categories that are permanently blocked when it is determined that they have no educational value and may be potentially harmful to users, these sealed categories include **offensive**, **illicit** and **extremism**. Blocked and sealed categories can also be set up with our **Lockouts** feature in which the Web Filter temporarily locks out users who persistently try to visit blocked web sites, disabling their Internet access for a configurable amount of time. Locked out users can be viewed and managed in the Lockouts report and an email can be sent to administrators to notify them that this has occured.

Violence.extremism Category

One specific Web Filter category that we have created to assist schools with the new act is the **violence.extremism** category. This category is populated with a list of web addresses that promote extremism and/or radicalization. This list is provided to Lightspeed Systems from The Home Office in the United Kingdom. The

Appendix 6