

Ditton Nursery School

E-Safety Policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

We understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named eSafety co-ordinator in our school is the Amanda Brown who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through: organisations such as Halton LA, CEOP (Child Exploitation and Online Protection), Cheshire Police (Channel co-ordinator, Counter Terrorism) and Childnet.

This includes having an awareness of and abiding by:

- Counter-Terrorism and Security Act 2015
- Prevent Duty Guidance 2015
- The Prevent Duty; Departmental advice for schools and childcare providers 2015
- Keeping Children Safe in Education 2016

Senior Management and Governors are updated by the Head or eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

eSafety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of regular staff training.
- Details of the ongoing staff training programme can be found in the School Development and Improvement Plan
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas thus helping children to begin to learn how to stay safe on line. Staff need to be aware of and vigilant to the risks posed by the online activity of extremist and terrorist groups, as outlined in the Prevent Strategy.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

ESafety in the Curriculum

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP report abuse button.

Password Security

- All staff users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Staff Users are provided with an individual network, email and Learning Platform log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Headteacher
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system and/or Virtual Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our school, all ICT password policies are the responsibility of the Headteacher and all staff are expected to comply with the policies at all times.

Data Security

The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008).

Staff are aware of their responsibility when accessing school data. They must not;

- allow others to view the data
- edit the data unless specifically requested to do so by the Headteacher.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Halton Internet Web Filtering Systems** is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by Halton Borough Council through its eSafety responsibilities.

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- **SMT raise awareness with all staff re appropriate websites for children to use and staff understand that they are to monitor the use of the internet and report any instances where children mistakenly view inappropriate sites to SMT**

INFRASTRUCTURE

Halton Local Authority has a monitoring solution where web-based activity is monitored and recorded.

- School internet access is controlled through the LA's web filtering service.
- The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.

NOTE for schools – the reference to Halton Local Authority and its web filtering systems is based on the school purchasing the relevant Council's web filtering SLA.

Managing other Web 2 technologies

Ditton Nursery school does not access networking sites with the pupils.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- The use of mobile phones and similar devices whilst on duty within the childcare environment is strictly forbidden
- Staff must ensure that personal mobile phones are not carried about their person during working hours.
- Personal mobile phones must be kept in lockers provided during working hours, although can be used during lunch breaks.
- Using a mobile phone to take pictures or video clips of children is not allowed
- Where trips are taken outside of the school staff may use a personal mobile, which is fully charged and switched on for the duration of the trip. This number is recorded on the Evolve form and employees are reimbursed for any use associated with the trip accordingly. The phone cannot be used for taking photographs.
- Pupils are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or emails between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff should not contact pupils outside normal school hours.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

School provided I-pads.

- Staff are allocated a numbered I-pad in order to use the 2 simple app for observation and assessment of individual children.
- All I pads are issued with an individual security password to unlock the I-pad.

- Staff may take photographs of the children on the camera in the I-pad but these photographs should be transferred onto 2-simple or nursery school laptops as soon as possible then deleted from the album. No children's photographs should be stored on the general I-pad album as occasionally staff take their I-pads home to complete and review observations.
- Access to print off children's records is only available through the master suite of 2 simple with a complex user name and complex password involving both letters and numbers.
- The Head Teacher as Senior Information Risk Owner will do occasional spot checks of the I-pads to ensure security is maintained.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives staff their own e mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- The forwarding of chain letters this includes jokes and funny statements. is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.

Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Consent of adults who work at the school

Permission to use images of staff who work at the school is sought for any photographs to be used in the public domain.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- in the school prospectus and other printed publications that the school may produce for promotional purposes
- on the school website
- digitally recorded
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. *Consent has to be given by both parents in order for it to be deemed valid.*

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- **Each key person** has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and CCTV

- We do not use publicly accessible webcams in school.

Video Conferencing

- We do not use video conferencing in school.

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety coordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children.

Parental Involvement

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by discussion through information events and annual questionnaires.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).

- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Posters
 - Website/ Learning Platform postings
 - Newsletters

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Ditton Nursery School

Acceptable Use Agreement: Staff, Governors and Visitors Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in School

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with the school eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head.
- I will not save any documents to a non-school PC or print to a non-school printer.
- I will not install any hardware or software without permission of the Head Teacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout Ditton Nursery School

Signature Date

Full Name(printed)

Job title

School Incident Log

'School name' eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Current Legislation (date)

Acts relating to monitoring of email

Users of this list should note that legislation is open to change and should always verify that the references and versions given or linked are up to date before relying on them.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hms0.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hms0.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any

monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information

www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The Prevent Duty June 2015

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

