KINDERGARTEN ONLINE SAFETY POLICY

INTRODUCTION

While new technologies are enhancing communication and creativity some are also challenging the definitions and boundaries of the school environment. As active participants in a digital world our broad curriculum and our children' personal goals requires regular use of a variety of IT systems and communication tools. While developments in technology may bring staff and children into contact with a wide variety of influences, some of which may be unsuitable, our kindergarten provides a progressive and appropriate education programme for staff, children and parents. Our aim is to provide children and staff with the knowledge, skills and confidence to become safe and responsible users of technology.

SCOPE

This Online Safety Policy relates to all members of the Thomas's community who have access to, and are users of IT systems and resources both in and out of school and applies to all electronic devices and services provided, whether accessed within school or an external location.

AIMS

The aims of this policy are to ensure that:

- staff and pupils are responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff and pupils are protected from potential risk in their use of ICT in their everyday work
- pupils, staff and parents are aware of the School's expectations and respect the privacy of all members of the school community

ROLES AND RESPONSIBILTIES

All Users

All users are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policy. All staff and pupils (including Principals) will sign an Acceptable Use Agreement and be trained in online safety. All users are expected to model safe, responsible and professional behaviours in their own use of technology.

Head / Designated Safeguarding Lead (DSL)

In the Kindergarten the Head is the Designated Safeguarding Lead. She is trained in Online safety issues and aware of the potential for serious safeguarding issues to arise inappropriate use of technology. It is important to emphasize that these are safeguarding issues, not technical issues, simply that technology provides additional means for safeguarding issues to develop.

The DSL's responsibilities are outlined in the Safeguarding and Child Protection policy. However with specific regard to online safety the responsibilities are as follows:

- To take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the kindergarten online safety policies / documents
- To be responsible for ensuring the safety (including online safety) of members of the kindergarten community
- To ensure that all new staff receive training and guidance in online safety as part of their induction
- To provide ongoing CPD to enable staff to carry out their online safety roles and to train other colleagues, as relevant
- To ensure that there is a system in place to allow for support of those in the kindergarten who carry out the internal online safety monitoring roles. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- To ensure that any online safety incidents are logged as a safeguarding incident and that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- To be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. The Safeguarding & Child Protection Policy section 'Dealing with allegations of abuse against staff' details the procedural steps to follow.
- To liaise with outside agencies e.g. Childnet, Police Community Support Officer
- To liaise with school IT technical staff on any online safety issues or concerns

Parents, carers and extended family

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet and online facilities in an appropriate way.

By signing the Kindergarten's Essential Child Information Form parents / guardians endorse the Kindergarten's Terms and Conditions which include reference to use of the Internet in Kindergarten and the use of digital images.

They will be encouraged to support the kindergarten by

- promoting good online safety practice
- following the Kindergarten's guidelines on the appropriate use of digital and video images taken at kindergarten events
- supporting and endorsing the guidance set out in this policy

Supply Teachers

- To receive the Staff Acceptable User Policy through the supply agency and coordinate with the Kindergarten Head who will give temporary login details, valid only for the length of time

they are working in the kindergarten, to access the kindergarten system for administration purposes.

Administrative Staff at Ringwood

- To ensure that new staff have signed the Staff Acceptable User Policy and forward the signed section to the Kindergarten Head.

EDUCATION STRATEGIES

Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety at an age appropriate level is therefore an essential part of the kindergarten's online safety provision. Children need the help and support of the kindergarten to recognise and avoid online safety risks and build their resilience.

Parents and Carers

To support parents in helping their children use technology safely the kindergarten will seek to provide information and awareness to parents and carers through:

- The Thomas's website and Kindergarten pages
- Letters, newsletters
- Parents' evenings
- Reference to relevant websites / publications
- Recommended guidance on technology use

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the kindergarten online safety policy and Acceptable Use Policies
- online safety issues will be announced to staff as appropriate in staff meetings
- Updates to this policy will be presented and discussed with staff in these meetings

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents / carers and children need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees. The kindergarten will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/children in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow kindergarten policies concerning the sharing, distribution and publication of those images. Those images should only be taken on kindergarten equipment, the personal equipment of staff should not be used for such purposes, unless the Head has given specific prior permission

Internal Use of images

Digital and video images may be used within the kindergarten for the purposes of display, celebration and kindergarten promotion. Examples of how digital photography and video may be used within the kindergarten include:

- children being photographed during activities and then displayed on the walls, in kindergarten books, on the digital photo frame and in their Leaning Journeys.
- presentations around the kindergarten to share good practice or celebrate achievements with other parents and teachers. (Taken from Appendix C of Staff Acceptable Use Policy)

External use of images

When photographs and videos are used for external purposes parents must be informed. Heads will inform staff as and when kindergarten events arise.

For any external use of digital images:

- if the child is named, we avoid using their photograph
- if their photograph is used, we avoid naming the child
- where showcasing examples of children' work we use only their first names
- if showcasing digital video work to an external audience, we take care to ensure that children are not referred to by name on the video and that children' full names are not given in the credits at the end of the film
- only images of children in suitable dress are used

Parents have given permission in the Kindergarten's Terms and Conditions for photographs to be included in kindergarten publicity. In exceptional circumstances the kindergarten may wish to post a picture of a child with their name on the kindergarten website, in these circumstances, written permission from parents or carers will be obtained before individual photographs are posted. On occasions parents may feature in photographs taking during school events. If their image is prominent in any photograph permission from the parent will be sought before using the photograph.

If an external organisation hosting a kindergarten trip requests pictures to be taken for their own publicity a consent form must be signed. (See Appendix 5 of this policy)

Video Conferencing/Streaming Video

When video conferencing is taking place parents must be notified beforehand by email or letter as this is streaming video and children will be informed about appropriate behaviour online and upholding the kindergarten's values.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Appendix 1 shows how the kindergarten currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

When using communication technologies the kindergarten considers the following as good practice:

- Users need to be aware that email communications may be monitored
- Any digital communication between staff employed by Thomas's and parents/ carers (email, chat, TLP, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Appendix 1 of the Kindergarten Staff Acceptable User Policy contains guidance for staff on the use of social networking sites, informing them that 'it is unacceptable to accept a friendship request from a child from school or from former children under the age of 20'. It further says: 'Staff are advised to exercise caution and discretion when accepting requests from parents of children or former children over the age of 18 as online friends'.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/Inappropriate Activities

Some Internet activity (e.g. accessing child abuse images or distributing racist material) is illegal and is banned from school and all other ICT systems. There are, however, a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities. Appendix 2 lists Internet usage restrictions within school

INCIDENTS

It is hoped that all members of the kindergarten community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, deliberate misuse.

An online safety incident is defined as a violation of the Staff Acceptable User Policy, described below or an incident involving technology that overlaps with child protection and safeguarding. Appendix 3 lists examples of possible online safety incidents and resulting sanctions.

Children should be regularly reminded to report anything they feel unhappy with and staff must act upon this according to the online safety procedures.

In the event of an accidental online safety incident, the Head must be informed to allow them to carry out an investigation.

Where the matter is not bullying but is a Child Protection issue, the Safeguarding Policy will be followed. The initial step is to refer the matter to the Designated Safeguarding Lead.

The Headteacher, the police and the Internet Watch Foundation will be informed in the case of illegal content found online.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above), they should follow these steps:

- The computer should be locked
- The Head is informed immediately and carries out investigation and determines action/sanctions to be applied.

In the event of suspicion of deliberate misuse the following procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the kindergarten community are aware that incidents have been dealt with.

MONITORING

The implementation of the online safety policy will be monitored by the Kindergarten Head. It will be developed in light of its success, significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Should serious online safety incidents take place, the kindergarten's Designated Safeguarding Lead will be informed, along with the Head and/or police and Local Safeguarding Board.

The kindergarten will monitor the impact of the policy using:

- an online safety events log
- parents/carers meetings
- questionnaires of staff

REFERENCES

See Appendix 5 of this Policy

See also: Anti-bullying Policy, Data Protection Policy, ICT (Acceptable Use) Policy, Mobile Phone (Acceptable Use) Policy, Safeguarding and Child Protection Policy, Whistleblowing Policy

This policy will be reviewed annually			
Latest Review: January 2017	By:	Kathy Ballantine, Acting Headmistress	No changes
Next Review: January 2018	By:	Joanna Copland, Vice Principal and Digital Leads	

Appendices

Appendix 1: Communications
Appendix 2: Internet Usage Restriction
Appendix 3: Examples of online safety incidents and resulting sanctions
Appendix 4: Permission form for external photographs
Appendix 5: Legislation

ONLINE SAFETY POLICY APPENDIX 1

COMMUNICATIONS

Communication Technologies that are accepted in kindergarten	Staff & other adults			Children		
	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed with staff permission	Not allowed
Mobile phones may be brought to kindergarten	✓				✓	
Use of mobile phones in lessons			✓			✓
Use of mobile phones in social time			✓			✓
Taking photos on mobile phones			✓			✓
Taking photos on camera devices			✓		✓	
Use of hand held devices eg PDAs, PSPs		✓			✓	
Use of personal email addresses in kindergarten, or on kindergarten network	✓				✓	
Use of kindergarten email for personal emails	✓				✓	
Use of chat rooms / facilities		✓				✓
Use of instant messaging		✓				✓
Use of social networking sites		✓			✓	
Use of blogs		✓			✓	
Use of forums	✓			✓		

ONLINE SAFETY POLICY APPENDIX 2

INTERNET USAGE RESTRICTIONS

The kindergarten believes that the activities referred to in the following section would be inappropriate in a kindergarten context and that users, as defined below, should not engage in these activities in kindergarten or outside kindergarten when using kindergarten equipment or systems. The kindergarten policy restricts certain Internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓
	criminally racist material in UK				✓
	pornography			✓	
	promotion of any kind of discrimination			✓	
	promotion of racial or religious hatred			✓	
	threatening behaviour, including promotion of physical violence or mental harm			✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the kindergarten or brings the kindergarten into disrepute			✓	
Using kindergarten systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the kindergarten				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the Internet				✓	
On-line gaming (educational)			✓		
On-line gaming (non-educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Use of video broadcasting eg Youtube			✓		

Incidents that constitute misuse of technology by staff/adults, and possible sanctions	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓		✓				✓
Inappropriate personal use of the Internet / social media / personal email	✓	✓				✓		
Unauthorised downloading or uploading of files	✓				✓	✓		
Allowing others to access kindergarten network by sharing username and passwords or attempting to access or accessing the kindergarten network, using another person's account	✓				✓	✓		
Careless use of personal data eg holding or transferring data in an insecure manner	✓					✓		
Deliberate actions to breach data protection or network security rules		✓			✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓	✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓			✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with children		✓	✓					✓
Actions which could compromise the staff member's professional standing		✓	✓					✓
Actions which could bring the kindergarten into disrepute or breach the integrity of the ethos of the kindergarten		✓					✓	
Using proxy sites or other means to subvert the kindergarten's filtering system	✓					✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓					
Deliberately accessing or trying to access offensive or pornographic material				✓			✓	
Breaching copyright or licensing regulations		✓						✓
Continued infringements of the above, following previous warnings or sanctions		✓					✓	✓

ONLINE SAFETY POLICY APPENDIX 4

PERMISSION FORM FOR PUBLICITY PHOTOGRAPHS

PARENT/GUARDIAN PERMISSION FORM FOR PUBLICITY PHOTOGRAPHS

I give permission for:

…… (child's name) in …… (form)

to have their photograph included with publicity material for:

…… (company or organisation name)

I understand that my child's name will not be used in connection with the photographs or if, for any reason this is required, additional permission will be sought.

Signed: …… (parent or carer)

Printed name: ……

Date: ……

ONLINE SAFETY POLICY APPENDIX 5

LEGISLATION

Kindergartens should be aware of the legislative framework under which this online safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Common Law Duty

Kindergartens have a common law duty of care to take reasonable steps to ensure that children and staff are safe from foreseeable harm.

Obscene Publications Act 1959 and 1964

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

Protection of Children Act 1978

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 a 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

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Computer Misuse Act 1990

This Act makes it an offence to:

- erase or amend data or programs without authority
- obtain unauthorised access to a computer
- "eavesdrop" on a computer
- make unauthorised use of computer time or facilities
- maliciously corrupt or erase data or programs
- deny access to authorised users

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Protection from Harrassment 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.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to other countries without adequate protection

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the kindergarten context, human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education

These rights are not absolute. The kindergarten is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- establish the facts
- ascertain compliance with regulatory or self-regulatory practices or procedures
- demonstrate standards, which are or ought to be achieved by persons using the system
- investigate or detect unauthorised use of the communications system
- prevent or detect crime or in the interests of national security
- ensure the effective operation of the system

Monitoring but not recording is also permissible in order to:

- ascertain whether the communication is business or personal
- protect or support help line staff

The kindergarten reserves the right to monitor its systems and communications in line with its rights under this act

The Education Act 2002, Sections 157 and 175

This places a duty on governing bodies of kindergartens to ensure the safety of children

Communications Act 2003

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.

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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Every Child Matters 2004

1. Be healthy
2. Stay safe
3. Enjoy and achieve
4. Make a positive contribution
5. Economic well-being

Children's Act 2004

(In addition to Every Child Matters)
Agencies working together to improve outcomes for children and young people.

Racial and Religious Hatred Act 2006

This Act makes it 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.

The Education and Inspections Act 2006 and 2011

Empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of children when they are off school site and empowers staff to impose disciplinary penalties, for inappropriate behaviour. Gave permission for Headteachers to search for electronic devices and data on electronic devices, as well as delete data.

Protection of Freedoms Act 2012

Kindergarten must seek permission from a parent to use Biometric Systems

The School Information Regulations 2012

Requires schools to publish certain information on its website.

Keeping children safe in Education 2015

Statutory guidance for schools and colleges giving advice on the safe recruitment of adults to work with children