Thelwall Infant and Nursery School
Online Safety Policy
2023

Content

Development, Monitoring, Review of this Policy

This online safety policy has been developed by a working group/committee made up of:

- Headteacher
- Computing subject leader
- Governors
- Consultation with the whole school community has taken place through the following:
- Staff meetings
- School/Student/Pupil Council
- Governors meeting/committee meeting
- School website

Schedule for Development, Monitoring, Review

This online safety policy was approved by the Full governers on: 20/11/23	Signed_____
The implementation of this online safety policy will be monitored by the:	*Headteacher* *Computing subject leader* *Governors*
Monitoring will take place at regular intervals:	*Termly*
The governors will receive a report on the implementation of the online safety policy as part of the headteachers report to governors which will include anonymous details of online safety incidents at regular intervals:	*Termly*
The online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*November 2024*
Should serious online safety incidents take place, the following external persons/ agencies should be informed:	*Gill Marsland (CEO)*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of
  - Pupils
  - parents/carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Governors:

The Governing board have overall strategic responsibility for filtering and monitoring.

Governors are responsible for the approval of the online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *online safety* Governor. Our online safety governor is Louise Simmonds (as part of the safeguarding governor role). The role of the online safety Governor will include:

- regular meetings with the safeguarding team
- regular monitoring of online safety incident logs
- reporting to Governors

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Computing subject leader*
- The Headteacher and another member of the Senior Leadership Team/Senior leaders will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see WBC flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/disciplinary procedures)

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Computing subject leader with Responsibility for online safety:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of online safety incidents via CPOMS
- meets regularly with online safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant Governor meetings
- reports regularly to Senior Leadership Team

Network Technician:

The DSL has responsibility for safeguarding and online safety, which includes overseeing and acting on:
• filtering and monitoring reports
• safeguarding concerns
• checks to filtering and monitoring systems

The IT service provider has technical responsibility for:
• maintaining filtering and monitoring systems
• providing filtering and monitoring reports
• completing actions following concerns or checks to systems

The IT service provider works with the senior leadership team and DSL to:
• Ensure that the school meets technical requirements including the DFEs filtering and monitoring standards (2023).
• procure systems
• identify risk
• carry out reviews
• carry out checks

ICT Technician is also responsible for ensuring:
• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
• that he/she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant, that the use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation/action/sanction.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read and understood the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Computing subject leader/ Headteacher
- digital communications with students/pupils (email on Google Classroom/Learning Platform) should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other school activities

- students/pupils understand and follow the school online safety and acceptable use policy
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of online safety issues related to the use of cameras and hand held devices and that they monitor their use.
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection/Child Protection Officer

should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students/pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- need to understand the importance of reporting incidents, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way by:

- endorsing the Pupil Acceptable Use Policy (child friendly rules)
- accessing the school website/Learning Platform in accordance with the Acceptable Use Policy.

Policy Statements

Education – students/pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety education will be provided in the following ways:

- online safety should be provided as part of ICT/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of assemblies and pastoral activities

- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Rules for use of ICT systems/internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through: Letters, newsletters, parent evenings and links to the CEOP web site and other relevant and appropriate online safety links on the school website.

Education & Training – 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 should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Computing subject leader will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA/WBC and others.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The Computing subject leader will provide guidance/advice/training as required to individuals as required

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any committee involved in ICT/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association or other relevant organisation.
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements

- School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software must be kept current.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password to access the school network
- All users of the school learning platform will be provided with a username and password for secure access in school and beyond.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
- The school uses securely as the managed monitoring and filtering service
- Any filtering issues should be reported immediately to the IT technician (and the DSL if necessary)
- Requests from staff for sites to be added or removed from the filtered list will be considered at the appropriate senior level.
- An agreement is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices**. (See appendix)**

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- Online safety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- online safety skills should be embedded through both discrete ICT and cross-curricular application.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images using school devices such as iPads, to support educational aims, but the sharing, distribution and publication of those images will only done with parental permission. Those images should only be taken on school equipment, the personal equipment of staff

should **not** be used for such purposes. All school equipment used for photograph/video must be password protected.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or Facebook page, and will never be used in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the GDPR regulations 2018 which state that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

Communications:

When using communication technologies the school considers the following as good practice:
- Where available the official school email service may be regarded as safe and secure and is monitored. Staff and students/pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc.) must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unkind words.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Remote Learning:

Online safety

This section of the policy is enacted in conjunction with the schools Remote Learning policy.

At the start of any period of home learning parents will be asked to remind their children of the school's online safety rules. These will be shared with parents as part of the home learning correspondence and can also be found on the school website.

All staff and pupils using video communication must:

- Ensure that when staff are participating in video calls with children that there is an adult present with them.
- Wear suitable clothing – this includes others in their household.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Not record, store, or distribute video material or any digital content without permission.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Always remain aware that they can be heard.

During the period of remote learning, and through computing lessons whilst in school, the school will maintain contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Responding to incidents of misuse

It is hoped that all members of the school 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, through deliberate misuse.
If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence. The CEO will be contacted regarding any misuse as described above and advice taken and acted upon. The Safeguarding Governor and Chair of governors will be informed that an incident has occurred.
(See flowchart in Appendix)
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as Actions & Sanctions-overleaf

Pupils Actions/Sanctions

Incidents:	Refer to class teacher	Refer to online safety Coordinator	Refer to HT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parent /carer	Removal of network/ internet access rights	Warning	Further sanction e.g. exclusion
Unauthorised use of non-educational sites during lessons	✓							✓	
Unauthorised use of digital camera/other handheld device	✓	✓						✓	
Unauthorised use of social networking/instant messaging	✓	✓				(✓)	✓	✓	
Unauthorised downloading or uploading of files	✓	✓				✓	✓	✓	
Allowing others to access school network by sharing username and passwords	✓	✓						✓	
Attempting to access or accessing the school network, using another student's/pupil's account	✓	✓				✓	✓	✓	
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	
Sending an message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓		✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		✓	✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		✓	

Staff Actions/Sanctions

Incidents:	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).	✓	✓	✓		✓	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓				✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓			✓	✓		✓
Careless use of personal data e.g. 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 instant 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 students/pupils	✓	✓			✓	✓		
Actions which could compromise the staff member's professional standing	✓	✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓			✓	✓		✓
Using proxy sites or other means to subvert the school'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	✓	✓			✓	✓		✓

Appendices

- Acceptable use Agreement for staff
- Parent/carer Acceptable Use Agreement/Permission form
- Pupils Acceptable Use policy- Child friendly online safety rules
- Appropriate use of removable media by students and supply teachers
- Remote learning
- Dealing with an online safety incident

Acceptable Use Agreement for all staff

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, learning platform etc) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will ensure the equipment used belongs to school and is password protected. Where these images are published (e.g. on the school website/Facebook page) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school when using my own personal equipment.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and ICT technician have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (e.g. mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate

or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as required to fulfil my role as class teacher.
- I will only use my encrypted removable media if personal data is transferred outside the secure school network.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name

Signed

Date

Parent/Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy (Child friendly online safety rules) is on our school website so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name

Student/Pupil Name

As the parent/carer of the above pupils, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed our online safety rules form and has received, or will receive, online safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed

Date

Pupils Acceptable Use Policy Agreement
(Child friendly online safety Rules)

- I will only use ICT equipment when I have been given permission to.
- When going on the internet I will only go on pages saved in the favourites or search for things I have been given permission to search for.
- I will never share my Learning Platform password with anyone else.
- I will always be kind and polite when sending messages.
- If I find anything I am not sure about on the internet I will hide the page and tell an adult straight away.
- I will always tell my teacher if something I am not sure about happens when I am on the computer.
- When using the iPads I will only use apps which are on the desktop.
- I will always ask permission before taking someone else's photograph or using someone else's photograph.

Signed _____ Date _____

Acceptable use agreement for Students and volunteers

Please DO NOT:

- download files onto the school computer systems
- Use a pen drive that does not have virus scanning technology
- Use own cameras/camera phones in school
- Take digital images or personal information about pupils out of school without permission from the Headteacher.

Signed_____ Date_____

Dealing with an online safety incident