IRCHESTER COMMUNITY PRIMARY SCHOOL

Online Safety Policy

Our e-safety policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard all adults and children within school. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within ICT.

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Data Protection, Security and our Curriculum statement.

Why have an e – Safety policy?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Cyber-bullying.
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing. Can potentially be widely distributed and publicly viewed.
- On-line content which is abusive or pornographic

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Roles and responsibilities of the school:

Governors and Head teacher

It is the overall responsibility of the Head teacher with the Governors to ensure that there is an overview of e-safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Head teacher has designated an e-safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-safety is addressed in order to establish a safe ICT learning

environment. All staff and students are aware of who holds this post within the school.

- Time and resources should be provided for the e-safety Leader and staff to be trained and update policies, where appropriate.
- The Head teacher is responsible for promoting e-safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Head teacher should inform the Governors at the standards and school improvement committee meetings about the progress of or any updates to the e-safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors are to be made aware of e-safety developments from the standards and school improvement committee meetings.
- The Governors **MUST** ensure Child Protection is covered with an awareness of e-safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An e-safety Governor (can be the ICT or Child Protection Governor) ought to challenge the school about having an e – safety policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:
  Challenging the school about having:
    - Firewalls
    - Anti-virus and anti-spyware software
    - Filters
    - Using an accredited ISP (internet Service Provider)
    - Awareness of wireless technology issues
    - A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures of the school.

E-safety Leader

It is the role of the designated e-safety Leader to:

- Appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that the e – safety policy is reviewed annually, with up-to-date information available for all staff to teach e-safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform or ensure the technician is informed and carries out work as directed. **(Filtering is set by Schools Broadband)**
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Head teacher on a regular basis.
- Liaise with the PSHE, Designated Safeguarding Lead (DSL) and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.

- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Transparent monitoring of the internet and on-line technologies – staff can access all pupil email accounts.
- Home use of school or setting equipment must be in keeping with this policy.
- Personal equipment may be used at school subject to appropriate electrical testing at work and used in keeping with this policy.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.
- Work alongside the ICT technician to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Head teacher and/or Governors.

Staff / Governors or other adults within the school

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the DSL is within school or other setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Head teacher. In the event of an allegation made against the Head teacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the head teacher lead immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the e-safety Leader.
- Alert the e-safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with e-safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- ***Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices. (This will vary from school to school, but is advisable so that there is staff protection against allegations made by children and young people.)***
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
  Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.

School business managers will need to ensure that they follow the correct procedures for any data required to be taken from the school premises. **(Encryption software on any equipment taken off site.)**

- Report accidental access to inappropriate materials to the e-safety Leader and learning platform helpdesk in order that inappropriate sites are added to the restricted list or control this via Schools Broadband.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/educational setting's network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.

Children and young people

Children and young people should be:

- Involved in the review of Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

Appropriate and Inappropriate Use

Staff / Governors or other adults within the school

- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
- They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- All staff should receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff.
- The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.
- When accessing the Learning Platform from home, the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.
- Please refer to appendices for a complete list of Acceptable Rules for Staff.

In the event of inappropriate use

- If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Head teacher immediately and then the Allegations Procedure (Section 12, LSCBN) and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

- In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

By Children or Young People

Acceptable Use Rules and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules will be on display within the computer suite.

Schools or educational settings should encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.
Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using the learning platform in or beyond school.

In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school, or in a setting, the following consequences should occur):

- Any child found to be misusing the internet by not following the Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the

screen or close the window. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. (Link available on all class page front covers.)

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Good Habits

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband for learning including the effective management of content filtering through Schools Broadband.
- National Education Network standards and specifications.

School e-safety Policy

The ICT Team will liaise with the DSL as the roles overlap to ensure e-safety procedures are in place.

Our e-safety policy has been written by the ICT Team using the Government guidance. It has been agreed by all staff and approved by governors after consultation with parents.

The e-safety policy will be reviewed annually, or more frequently as required, to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. The following concepts, skills and competencies should have been taught by the time they leave *Year 6*:

- Internet literacy

- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

We use the www.thinkuknow.co.uk resources for KS1 and KS2, within ICT to teach responsible use of the internet, emails and keeping safe.
Teachers and pupils may use the internet outside school for personal and educational use. In order to ensure their own safety and security it is essential they understand and abide by the school e-safety rules.

Pupils with additional learning needs
The school or setting should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Filtering

The school will work in partnership with the Local Authority and Schools Broadband (Internet Service Provider) to ensure filtering systems are as effective as possible.

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator or network manager, who will then ensure the ISP is informed immediately.
- Social networking sites and newsgroups are blocked for pupil use via the filtering system.

Learning Platform
The DB learning platform provides a wealth of opportunity for adults and children within and beyond school to:

- collaborate and share work via uploading
- ask questions
- debate issues
- dialogue with peers
- dialogue with family members or carers
- access resources in real time
- access other people and cultures in real time
- develop an on-line community

The tools available for use within the learning platform for adults and children include:

- Internet access

- E-mail
- Weblogs (on-line diaries)
- Wikis (on-line encyclopaedia or dictionary)
- An on-line personal space for adapting as a user to:
    - upload work
    - access calendars and diaries
    - blog

Any personal space will contain some information about the user. These areas should be used as an opportunity to discuss with children and young people appropriate information to enter to **ANY** website asking for personal details (such as a social networking site e.g. Bebo and Facebook) and should reflect key messages for any on-line use.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any websites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

Safety

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will not access the internet unsupervised.

- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised frequently on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Mobile phones will not be used by pupils in school.
- Children should use a search engine that is age appropriate. Appropriate child friendly search engines will be linked on class pages within the DB platform.
- If the children see something or search for something that is inappropriate they are taught how to deal with this…turn off the screen/minimise the screen and report to the adult in charge of the session. The adult then passes this information on to the e-safety lead to log and take further with schools broadband as a filtering issue.

E-mail

The school will have individual E-mail addresses for children to use as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual E-mail accounts can be traced if there is an incident of misuse.

Staff, governors, children and young people should use their school issued e-mail addresses for any communication between home and school only. A breach of this may be considered a misuse and will result in consequences.

Parents/carers are encouraged to be involved with the monitoring of e-mails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of e-mails where there are communications between home and school/setting, on a regular basis.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- If pupils send work to staff by email it must be via Learning Platform accounts, and if staff reply it must only be to Learning Platform accounts as they can be monitored for safety of both staff and children.

Mobile Phones

Staff/governors **will not** use personal mobile phones to take pictures or record video of any of the children. If photos or video are needed, whether it be on school premises or trips/visits, then school has digital cameras or tablets to use.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material (e.g. supervision/correct filtering levels set by Schools Broadband). However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

Teaching and Learning within ICPS

- All current staff, governors and pupils are automatically granted Internet access.
- All staff and governors must read and sign the ‘staff code of conduct’ before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.
- Pupils will be asked to sign internet and email rules with parents.
- Internet access will be planned to enrich and extend learning activities.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- School will ensure that the use of Internet derived materials by pupils and staff and governors complies with copyright law.

- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Personal Use

It will be possible to access learning platforms at home, but we would advise parental supervision and regular reminders to follow the safety guidelines as taught in school.

Published Content and the School Web Site

- The contact details on the Web site should be the school address and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, unless there is prior parental agreement.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Annual written permission from parents or carers will be obtained before photographs of pupils' and their work are published on the school Web site.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulation.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure as outlined in the school brochure.

- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Social networking advice for staff and governors

Social networking outside of work hours, on non school-issue equipment, is the personal choice of **all** school staff/governors. Owing to the public nature of such websites, it is advisable for all to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with current students or past students outside of Head teacher authorised systems (e.g. school email account for homework purposes)
- Irchester Community Primary School advise all staff members who are participating in social networking to activate the highest level of privacy settings possible on their profiles to prevent unsolicited contact by current and past children or parents. **Staff/ governors will ensure that their online activity, both in the school setting and outside, will not bring their professional role into disrepute.**
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students)
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Some schools and other educational settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include EdModo or Virtual Learning Environments such as Moodle which contain similar features.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored and should not be unsupervised.

Staff

- **All** staff/governors have access to the School e-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. **Discretion and professional conduct is essential.**

Parents

- Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure, school website and through the e-safety rules letter.

APPENDICES

Staff Procedures following misuse by staff – Appendix A

Staff Procedures following misuse by Children – Appendix B

Acceptable use rules for staff, governors and visitors – Appendix C

e-safety Acceptable Use Rules Letter to Parents/Carer for Primary – Appendix D

E-safety Rules– Appendix E

Staff Code of Conduct – Appendix F

Staff e-mail policy – Appendix G

Using all computers/laptops in school – Appendix H

Appendix A - Staff Procedures Following Misuse by Staff

The Head teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report website to the e-safety Leader if this is deemed necessary.

Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Head teacher and e-safety Leader immediately.
Head teacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Head teacher immediately.
Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Head teacher and / or DSL immediately, who should then follow the Allegations Procedure and Safeguarding Policy.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Head teacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Head teacher or Chair of Governors (if allegation is made against the Head teacher) and / or DSL immediately and follow the Allegations procedure and Safegaurding Policy.
Contact CEOP (police) as necessary.

F. Threatening, malicious, unkind, or hurtful comments are posted to the school website, learning platform, or a social networking site (or printed out) about a an adult in school/ a school situation:
Preserve any evidence.
Inform the Head teacher immediately and follow Safeguarding Policy as necessary.
Inform the RBC/LA/LSCBN and e-safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

G. Where staff or adults are posting on inappropriate websites or have inappropriate information about them posted this should be reported to the Head teacher.

Appendix B - Staff Procedures Following Misuse by Children

The Head teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the e-safety Leader if this is deemed necessary.

Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform LA/RBC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Head teacher and / or DSL immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Head teacher must follow the Allegation Procedure and/or Safeguarding Policy.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Head teacher immediately.
Inform the e-safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Head teacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.
If in doubt, do not power down the machine.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Safeguarding Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the DSL is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this

constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix C - Acceptable Use Rules for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Head teacher, and / or DSL or e-safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who the DSLs are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Head teacher and/or e-safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-safety Leader.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed……..Date…….
Name (printed)…….

e-safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs
I agree that my son/daughter's work may be electronically published on the secure school website/ learning platform. I also agree that appropriate images and video that include my son/daughter may be published.

Signed:	**Date:**

Parent's Consent for Internet Access

- ✓ I will encourage my child to keep their password private (but they may tell me).
- ✓ I will tell a member of staff if I think that someone else knows their password.
- ✓ I will encourage my child to be a responsible user of the Learning Platform and to use appropriate language when he/she adds items or sends e-mails.
- ✓ I will encourage my child to act responsibly by telling a member of staff if they think that someone else has broken the rules.
- ✓ I will ensure adequate supervision and responsible use of the internet at home.
- ✓ I will ensure my child knows to tell either myself or staff members if they see or read inappropriate material on the internet.
- ✓ I understand that access to the Learning Platform is provided by the school and all users must adhere to the user agreement in order to retain log-in privileges.
- ✓ I understand that if my child does not keep to the rules, I will be informed and my child will not be allowed to log-in to the Learning Platform or use the school internet for a set period of time (decided by the Head teacher).
- ✓ I understand that the school will take all reasonable precautions to ensure my child cannot access inappropriate materials but I appreciate that this is a difficult task. I understand, therefore, that the school cannot be held responsible for the materials accessed through the internet.
- ✓ I understand that by signing this agreement I am giving permission for my child to use the internet in school and to have access to the Learning Platform.

Signed:	**Date:**

Parent's Consent for E-mail Access in school and at home, in line with the home school agreement

I give permission for my son/daughter to access school e-mail via the learning platform at school and home.

Signed:	**Date:**

Please print name:

Name of child: **Class:**

Please complete <u>both sides of this form</u>, sign and return to the school

Appendix E - FOUNDATION STAGE & KEY STAGE 1

These are our rules for using the internet safely and responsibly.

Our Internet and E-mail Rules

- We log on to the internet via the DB Platform.
- We learn how to use the internet.
- We use the internet safely to help us learn.
- We use safe search engines, which are on our class pages, to carry out any research on the internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We understand that everything we do on the DB Primary Platform can be seen by our teacher.
- We only use school email addresses for school related work.
- We only tell people our first name.
- We learn not to give our password to other children/people.
- We know to ask an adult if we need help.
- We promise to turn monitors off if we see anything that upsets us and report it to an adult.
- We know that it is important to follow the rules.
- We must always log off the computers when we have finished our work.
- We are able to look after each other by using our safe internet.
- We can go to <u>www.thinkuknow.co.uk</u> for help.

I agree to follow these e-safety rules when using the internet and email.

Name of child _____ Date _____

Class _____ Signature of parent

_____

Key Stage 2

These are our rules for using the internet safely and responsibly.

Our On-line Rules

- We log on to the internet via the DB Platform.
- We understand that everything we do on the DB Primary Platform can be seen by our teacher.
- We use the internet to help us learn and we will learn how to use the internet safely and responsibly.
- We use search engines, which are on our class pages, to carry out any research on the internet.
- We send e-mails and messages that are polite and friendly.
- We only use school email addresses for school related work.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips without permission and never include names with photographs.
- If we need help we know to ask an adult.
- If we see anything on the internet or in an e-mail that makes us uncomfortable, we turn the screen off and tell an adult immediately.
- If we receive a message sent by someone we don't know we do not open it and we tell an adult immediately.
- We know we should follow the rules as part of the agreement with our school/parent/carer.
- We must always log off the computers when we have finished our work.
- We are able to look after each other by using our safe internet in a responsible way.
- We know that we can go to www.thinkuknow.co.uk for help.

I agree to follow these e-safety rules when using the internet and email.

Name of child _____ Date _____

Class _____ Signature of parent

_____

Appendix E –

IRCHESTER COMMUNITY PRIMARY SCHOOL

e-safety Rules

These e-safety Rules help to protect pupils and the school staff by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to teaching and learning.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer

system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix F - Staff/Governor Information Systems Code of Conduct

To ensure that staff/governors are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-safety Coordinator or a Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils/parents are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not post pictures or comments on social networking sites that bring the school into disrepute.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Appendix G - Policy for Email Use in School for Staff and Governors

1. **Email Benefits**

   An email account allows staff to facilitate communications with the LEA advisory staff and support services, professional associations and colleagues.

2. **Email Use**
   - **Staff are allowed to access personal email with their school account provided the following conditions are adhered to.**

3. **Appropriate Use**
   - **Staff need to be aware that emails are easily forwarded so be professional and careful about what you write.**
   - **The downloading and sending of copyright material is prohibited.**
   - **None of the following should be deliberately sent:**
     [i] Pornographic language
     [ii] Pornographic pictures
     [iii] Information which may be considered offensive or threatening to others
     [iv] Defamatory or illegal information

4. **Standards**
   - **Emails should only be read by the intended recipient.**
   - **Staff should open their email a minimum of three times a week**
   - **A signature should be added to any email sent. This should include your name, position, Irchester Community Primary School and school phone number in addition to the disclaimer as stated below:-**

   "*This email and any files transmitted with it are confidential and intended solely for the use of the named recipient. If you have received this email in error please notify* Irchester Community Primary School *and/or sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Irchester Community Primary School. Finally, the recipient should check this email and any attachments for the presence of viruses. The sender accepts no liability for any damage by any virus transmitted by this email."*

5. **Security**
    - **Staff should keep their password confidential and it should not be disclosed under any circumstances.**
    - **Staff should change their password occasionally.**
    - **Staff may only use their own password protected accounts to send and check email.**
    - **Sensitive information should be sent by post or via a secure transfer system.**
    - **Certain emails may need to be printed.**
    - **Staff must not leave their mailbox open and unattended.**

6. **Safety**
    - **Only register your email address with reputable organisations**
    - **Never give personal details out over the internet unless you have initiated the transaction and you are confident of the identity of the receiving party.**
    - **Never open, reply or forward spam [junk mail]**
    - **Staff who receive inappropriate email need to inform the head immediately; the email must not be replied to.**
    - **Follow the school guidelines to ensure that the anti-virus on your PC is kept up-to-date.**
    - **Be cautious when opening attachments; save any attachments to the computer's hard drive to ensure they are scanned before opening.**
    - **Report any problems with your email account to the ICT co-ordinator for resolution.**

7. **Sanctions**
    - **The head teacher will be responsible for ensuring that this policy is implemented effectively.**
    - **Deliberate misuse of email will result in disciplinary action taken against you.**

I have read the list of email statements above and I accept them.

Staff Name=
Staff Signature=
Date=

Policy for Email Use in School

Administrator Agreement

- **I will not access any email accounts without first seeking agreement from the Head teacher.**
- **On occasions emails may be redirected to the school email administrator, I will handle these with confidentiality, unless the head teacher needs to be informed.**

Staff Name=
Staff Signature=
Date=

Appendix H – Using computers/laptops in school

- Teachers must log on using surname and then first initial and then password already set.
- Teachers – when/if leaving work for supply – you must leave this work on the dedicated drive for supply staff as this is what they will access.

- For all TA's/other staff/governors/visitors – please only log on to **staff use** only computers with your username and the password 'red'
- When you log on for the first time you will be asked to change the password to something you will remember – do not share the password.
- All teachers have a laptop which is set up for staff use
- Staff should contact the IT technician to access other staff use computers

- Please **do not** log on to any lap top/computer not saying staff use.

- Supply staff – please use the **staff use** only laptops and the username 'supply' password 'supply'. Then please use the dedicated drive on the network for supply staff.

- **If in any doubt please check before logging on.**