

Riverside School

E-Safety Policy



Date of this Review	Summer 2026
Review cycle	3 years
Date of next review	Summer 2029
Full Governing Body	

This policy should be read in conjunction with other documents such as:

- *Safe Schools, Safe Children, Safe Staff (Code of Conduct)*
- *Keeping children safe in education: information for all school and college staff*
- *Using Facebook Safely*

We at Riverside school believe that E-Safety is the responsibility of the whole school community, and everyone has the part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The aims of this policy are as follows:

To create and maintain a safe ICT learning environment for all pupils, staff and visitors.

- To define the different types of digital technology and the risks they present to children;
- To provide guidance to all staff, pupils, volunteers, parents/carers and visitors regarding the safeguards that are in place to protect children using digital technology, whatever the setting;
- To provide information about some risk indicators in relation to the internet and digital technology;
- To provide guidance to all staff, pupils, volunteers, parents/carers and visitors as to what action they should take if they are concerned about a child or young person related to digital and interactive technology, and provide information about legislation;
- To provide guidance to all staff, pupils, volunteers, parents/carers and visitors about how to minimise risk for themselves, so that they do not inadvertently leave themselves open to allegations against all staff, pupils, volunteers, parents/carers and visitors misconduct from children or their parents / carers.
- To provide information about legislation.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone in the school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

Managing ICT Systems and Access

- The school will be responsible for ensuring the access to the ICT systems is as safe and secure as is reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, Workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.

The School will take reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.

Filtering Internet Access

- The School uses a filtered internet service.
- If users discover a website with inappropriate content, this should be reported to a member of staff, the Computing Subject Leader and the ICT Manager.
- If users discover a website with potentially illegal content, this should be reported immediately to the Computing Subject Leader, ICT Manager and the Head teacher. The school will report this to the local authority.
- Internet sites can be blocked internally using software located on the server, this software can block software from pupils but staff can still access the websites if required.
- The School will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Email

- Staff should use approved email accounts allocated to them by school, and be aware that their use of the school email system will be monitored and checked.
- Staff are not permitted to access personal email accounts during school time.
- Communication between staff or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using Images, Video and Sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will be created using equipment provided by the school.
- In particular, digital images, video and sound will not be taken without the permission of the participants; images and video will be of appropriate activities and participants will be in appropriate dress. Full names of participants will not be used either within the resource itself, within the filename or in accompanying text online; such resources will not be published online without the permission of the pupils involved, their parents/carers and involved staff.
- If pupils are involved, relevant parental permission will be sought before resources are published online. Relevant permissions are sought from parents/carers on admission.

Mobile Phones

- Pupils may not use mobile phones whilst at school. Pupils will be required to either hand them over to a member of staff for secure storage.
- Personal mobile phones will only be used in lesson with permission of the teacher and for specific, agreed purpose.
- Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff.
- Where staff members are required to use mobile phone for school duties, for instance in case of an emergency during off-site activities or for contacting pupils or parents, then a school mobile should be provided and used. Staff mobile phones may be used as additional “back-up” when on educational visits, etc.
- Staff will not be expected to use personal mobile phones in any situation where their phone number or other personal details may be revealed to a pupil or parent.
- Staff must not use their mobile phones to record photographic images of pupils.
- All visitors are required to turn their mobile phone **off** on entry into school or switch to silent.

Use of tablets

Day to Day Use:

Each class teacher will be provided with an Apple iPad tablet, a wall socket, a charging lead and a case. In addition to this each class has an additional class iPad, which travels around school with the class for all subject teachers and LSA's to use i.e. take photographic evidence of work, complete assessments. These items remain the property of Riverside School and should not be loaned out to individuals not associated with the school. We understand that all the items will be subjected to general wear and tear but expect the devices to be well cared for. All devices should be left in a secure location when not in use. The devices are controlled by the I.T. Manager. This software enables the IT department to deploy apps and impose restrictions on the devices. It can also be used to locate lost devices. If you lose your device, you need to contact the IT department so they can remotely wipe / lock your device. Employees are provided with tablets to make their assessment more efficient and to also be able to communicate more effectively with parents. To this end, we have preloaded BSquared and DoJo onto each device. Staff email accounts can be linked to the devices to make it easier to read and respond to emails.

In the unlikely event that staff have accessed materials that are not related to school it is their responsibility to clear the browsing history on their device before coming back to school. (Advice for this can be found online) If technical difficulties occur, the IT department will use the "10-minute" rule. If the problem cannot be fixed in 10 minutes, the tablet will be restored to factory defaults. Re-imaging will restore the device to the state in which the user originally received it. All files on the tablet will be lost in this instance which is why it is imperative to back up data regularly. Managing Your Files and Saving Your Work: Employees may save files to the tablets internal memory. It will be the responsibility of the employee to maintain the integrity of their files and keep proper backups. Employees will also be responsible for maintaining the amount of space used on their device. All work/photos saved on the device will remain on the device as the school will not be using any web based storage facilities such as icloud or dropbox. If photos or files are needed they can be downloaded to the school network. (Please see online for support if needed)

Software on Tablets:

Originally Installed Software:

The software originally installed on the tablet must remain on the tablet in usable condition and easily accessible at all times. From time to time the school may add software applications for use by teachers. This will enable the tablets to be tailored to the individual's needs. This process will be automatic and will require no action on the user's part. Applications that are no longer needed will automatically be removed by the school as well. Additional Software: Employees are unable to install additional software on their tablet. If employees would like any specific apps or software they should speak to the IT department.

Acceptable Use: The e-safety policy applies to the usage of the tablets.

Repairing or Replacing Your Tablet: iPad Warranty:

This coverage is purchased by the Riverside School as part of the price of the tablet. Apple warrants the tablet from defects in materials and workmanship. This limited warranty covers normal use, mechanical breakdown, or faulty constructions and will provide replacement

parts necessary to repair the tablet or tablet replacement. The Apple warranty DOES NOT warrant against damage caused by misuse, abuse, accidents, or computer viruses. Please report all tablet problems to the IT department.

Lost, stolen, or lost in fire:

A tablet that is lost, stolen, damaged, or lost in a fire is the responsibility of the employee involved in the loss of property. Upon reporting the lost/theft of a device the IT department will attempt to locate the device through GPS, if that is possible the IT staff may be able to remotely lock/wipe the device to safeguard any material. A police or fire report must be filed by the employee involved in the loss of property. A copy of the report must be brought to the Head of IT. The user will not be given another tablet to use until the matter is resolved.

Using New Technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.
- We will regularly amend the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safety risk.

Protecting Personal Data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998
- Staff will ensure they properly log-off from a computer terminal after accessing personal data. If leaving a computer unattended which is displaying or allows access to personal and/or confidential information, staff must either “lock” or shut down the machine.
- Staff will not remove personal or sensitive data from the school premises without permission from the headteacher, and without ensuring such data is kept secure.
- Staff must not copy digital information to portable devices (eg flash cards/memory sticks, portable hard drives,) unless password protected or encrypted.

GDPR

GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be

taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Minimising Risk:

One of the most important messages that we should ensure children understand in relation to using digital technology is that they should not give out personal information, particularly their name, address or school, mobile phone numbers to anyone they do not know or trust. This particularly includes social networking and online gaming sites. If they have been asked for such information, they should always check with their parent or other trusted adult before providing such details. It is also important that they understand why they must take a parent or trusted adult with them if they meet someone face to face who they have only previously met on-line.

Educating children to behave responsibly and safely online is the responsibility of parents or carers and all those working with them when using computers, whether that be in schools, youth clubs, residential children's homes, home education service etc. Firewalls and filtering software alone will not protect them; we need to supervise their activities and give advice and guidance to ensure they have a safe online experience.

Ten Steps to Minimise Professional Risk

You should fully appreciate that the onus is upon you and not the child or young person to distance yourself from any potentially inappropriate situation;

- Review all content about yourself on social networking sites, such as FaceBook, Snapchat etc. Particularly consider removing any personal information or photographs. These could be manipulated and used against you;
- Do not give personal information such as email addresses or mobile telephone numbers including pin numbers to anyone who is, or has been, a pupil, or is a member of their family;
- If you wish to keep in contact with any child or young person under the age of 18, or their family, who has been a user of your service, ensure that you only use work emails or telephone numbers to communicate with them and that your manager is aware of the contact;

- If there is any incident, related to this guidance, which involves a child, young person or their family, that causes you concern, report it immediately to the E-safety co-ordinator/Designated Safeguarding Lead/Head teacher. Document it as soon as possible, according to your workplace procedures;
- Ensure you adhere rigidly to the E-safety policy and Staff Acceptable Use Policy of your workplace. If you breach any part of the Acceptable Use Policy, report it immediately as per your workplace procedures;
- Do not access any illegal or inappropriate websites on your personal computer/laptop or mobile phone. This includes illegal or inappropriate images of children, certain other types of pornography or extremist websites. It is illegal to access or download material that promotes or depicts criminal behaviour;
- Be very careful when liaising with others online (for example in chat rooms, message boards, forums, social networking sites and newsgroups). Remember these are not private areas even though you may have privacy settings applied so comments or complaints may be seen by others. Avoid inappropriate communication with individuals under 18, or with who you may be in a position of trust;
- Use your common sense and professional judgement and expertise at all times to avoid circumstances which are, or could be, perceived to be of an inappropriate nature or which could bring your school into disrepute. This relates particularly to social networking sites and mobile phone technology;
- Remember, digital technology and social media may be the virtual world, but it has an impact on our real world. Online actions can have offline consequences.

See **UK Safer Internet website** and CEOP, **thinkUknow website**.

Supporting Parents to Safeguard their Children

We need to ensure that those who care for children are equipped with the knowledge and understanding of how to keep them safe and what to do if things go wrong.

Often parents do not use these environments and therefore lack confidence in supervising their children's online activities. It is important that we support parents by raising awareness of the benefits, risks and dangers to help them understand more about what their children are doing online. We need to offer practical advice and guidance on how to keep their family safe online and what to do if things go wrong.

See **thinkUknow website**.

Procedures for Reporting Concerns:

Any concern around e-safety should be reported appropriately and immediately, staff will complete the e-safety concern form and give it to the ICT coordinator (see Appendix 1)

At any time there is concern that an offence has been committed, or a child or young person is at risk due to their, or another's, use of digital or interactive technology, the following steps should be taken:

If a worker is concerned that a child is at risk of **Significant Harm**, a telephone referral must be made as soon as possible to Children's Social Care: see **Local Contacts**.

In an emergency, ring 999 to contact East Yorkshire Police.

If a practitioner believes a child has additional needs or is a child in need, but is not at risk of Significant Harm, they should refer them to the Multi-Agency Support Team (MAST) in the appropriate Service District. The MAST will undertake a EHA(Early Help Assessment), refer them to the Interim EHA Panel / Allocation Panel, and as a result appropriate support services will be put in place for the child and their family, in order to improve their outcomes. See **Local Contacts** for contact details for each of the Service Districts offices.

If your concern is about cyberbullying, commercial exploitation, inappropriate or illegal content of website's etc., but you do not think a child or young person is at risk of Significant Harm, then you should ring **East Yorkshire Police** and ask to speak to the relevant Safer Neighbourhood Team, to report the incident/s.

You can obtain advice about safeguarding concerns in relation to digital or interactive technology from **East Riding Safeguarding Children Advisory Service**.

Online safety help for professionals is available from the UK Safer Internet Helpline **helpline@saferinternet.org.uk**. Telephone 0844 381 4772

Online help and reporting of sexual exploitation is available through the **Child Exploitation and Online Protection (CEOP) Advice, Help and Support Centre**.

Children's protocol: (Taken from E-safety rules poster-Appendix 2/3)

What to do if you are worried/concerned...

- Tell your teacher
- Your teacher will tell the DSL and sort the problem from there

Guidance for professionals to Minimise the Risk of Misconduct Allegations related to Digital and Interactive Technology

This is guidance that relates specifically to helping professionals put safeguards in place to minimise the risk of any allegations of professional misconduct related to the use of digital technology and social media (e.g. Social networks such Facebook, LinkedIn, online gaming, etc.). The school also follows the East Riding policy of staff use of social media guidelines.

This guidance relates to all children up to the age of 18, whether or not they, or their families, are current or former pupils. It is appreciated that you may have personal friends or the children of friends who are under the age of 18. But at all times you should ensure that you treat all those under the age of 18 with the respect they deserve, whoever the child or young person is.

You should always be mindful not to put yourself in a situation that may comprise you or be misinterpreted either by the child or young person, their friend, parent or carer, or any other person. This includes both personal and professional situations. It is remembered that careless and inappropriate action in a personal setting, whether intended or not, could have significant implications for your professional life.

There are few professionals who have allegations of professional misconduct related to digital technology or social media made against them. However, the impact of either an allegation or cyberbullying can be significant, both personally and professionally. Taking a few steps to be pro-active in minimising any risk to yourself, whilst you may think it unnecessary, is worth taking to avoid future complications.

Remember: as a professional working with children or their families, you may be vulnerable to have an allegation made against you or being the victim of cyberbullying. Sometimes this is a result of communication or a situation being misconstrued. Other times this may be an act of revenge taken against you for an incident that has resulted through your professional practice. It may also be that someone, through having complex needs of their own, may develop an unhealthy interest in you as a person.

Therefore the following steps are recommended to all professionals, and trainees who are or will be working with children or their families.

Social media

SOCIAL MEDIA DEFINITION

Social media technologies take on many different forms including magazines, Internet forums (message boards), weblogs (blogs), microblogging (Reddit), social networks (Facebook etc), podcasts, photographs or pictures, video and virtual game worlds (Moshi Monsters, Club Penguin, etc). **WEBSITES AND BLOGS** The following guidelines apply:

- Staff, governors, parents and carers must not disclose any information that is confidential to the school or any third party that has disclosed information to the school.
- Staff, governors, parents and carers should not link any personal websites, social networking sites etc to the school's website.

Staff, governors, parents and carers must not use the school website, internet systems, e-mail addresses or intranet for their weblog and staff must not write their weblog in employer time. If a member of staff, governor, parent or carer is asked to contribute to an official weblog connected to the school, then special rules will apply and they will be told in detail how to operate and what to write.

The school uses social media platforms which are monitored and maintained by the IT Manager and the E-Safety/ICT subject leader. Any negative comments on posts will be deleted.

Riverside School will not tolerate criticisms through social media websites and blogs. If a member of staff feels aggrieved, then they must follow the procedures outlined in the Complaints and Whistleblowing Policy.

SOCIAL NETWORKING SITES

The school respects a member of staff's right to a private life. However; the school must also ensure that confidentiality and its reputation are protected.

The school expects all staff, governors, parents and carers to:

- Ensure that they do not conduct themselves in a way that is detrimental to the school.
- Take care not to allow their interaction on these websites to damage working relationships between members of staff and clients of the school.

IMPORTANT CONSIDERATIONS

When writing a weblog and placing information on social networking sites, staff, governors, parents and carers should follow these guidelines:

- Do not include any information that breaches copyright and should link to other material rather than cutting and pasting it

- Do not defame (libel) anyone. A member of staff, governor, parent or carer who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned
- Include personal information about an individual without his/her consent, otherwise they risk breaching the Data Protection Act 1998, which is a criminal offence
- Include material that is abusive, defamatory, sexist, racist or that could be interpreted as harassment or bullying
- Bring Riverside School into disrepute
- Staff should only access social media sites in their own time
- Staff should not comment on any posts made by others relating to the school
- Staff should not share or discuss matters relating to the school
- It is not advisable to invite parents/carers to become your friends on social networking sites. There may be a conflict of interest and security and privacy issues, but where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the teacher's code of conduct
- Staff should not accept friend requests from Riverside pupils under any circumstances
- Staff should use the privacy settings available
- Staff should not share personal conversations.
- Staff should behave respectfully and should not engage in topics that may be considered objectionable or inflammatory such as politics or religion

PERSONAL USE OF THE INTERNET

Riverside School does not allow personal use of the internet during session times.

DISCIPLINARY ACTION

If necessary, action will be taken against any member of staff, governor, parent or carer who is found to have breached this Policy. Staff should also refer to the Disciplinary Policy.

SECURITY AND IDENTITY THEFT

Staff, governors, parents and carers should be aware that social networking websites are a public forum, particularly if they are part of a 'network'. Staff, governors, parents and carers should not assume that their entries on any website will remain private. Staff, governors, parents and carers must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and, for example, favourite football team which can form the basis of security questions and passwords.

Cyberbullying

Policies and procedures

Ensure regular review and update of existing policies to include cyberbullying where appropriate. Riverside will keep good records of all cyberbullying incidents. Adults to log all incidents with the Head or Assistant Heads Designated safeguarding officers). The IT technician will use filtering, firewall, anti-spyware software, anti-virus software and secure connections to safeguard the pupils. Though electronic controls alone can never be 100% effective, and pupils should adhere to the local authority guidelines.

Promoting the positive use of technology Riverside will;

- Make positive use of technology across the curriculum
- Use training opportunities to help staff develop their practice creatively and support pupils in safe and responsible use
- Ensure all staff and children understand the importance of password security and the need to log out of accounts Making reporting easier
- Ensure staff can recognise non-verbal signs and indications of cyberbullying with regular safeguarding training.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.
- Publicise to all members of the school community the ways in which cyberbullying can be reported.

- Provide information for all students including reassurances about 'whistleblowing' and the appropriate way of informing appropriate staff or parents about incidents they have witnessed
- Provide information on external reporting routes e.g. mobile phone company, internet service provider, Childline, CEOP or the NSA Evaluating the effectiveness of prevention measures
- Identify areas for improvement and incorporate pupil ideas derived from School Councils
- It is desirable to conduct an annual evaluation including a review of recorded cyberbullying incidents.

Responding to cyber bullying

Most cases of cyberbullying will be dealt with through the school's existing Anti-bullying Policy and this must remain the framework within incidents of bullying are investigated. However, some features of cyberbullying differ from other forms of bullying and may prompt a particular response.

The key differences are:

- impact: the scale and scope of cyberbullying can be greater than other forms of bullying targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets
- location: the 24/7 and anywhere nature of cyberbullying
- anonymity: the person being bullied will not always know who is bullying them
- intent: some pupils may not be aware that what they are doing is bullying
- evidence: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence
- it is possible that a member of staff may be a victim and these responses apply to them too

Roles and responsibilities:

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

Governors:

Governors are responsible for the approval of the E-Safety policy and for reviewing its effectiveness. They will receive regular information and monitor any incidents relating to E-Safety. A member of the Governing Body has been appointed the role of the E-Safety Governor: Helen Caldwell

The role of the E-Safety Governor will include:

- Regular monitoring of e-safety incidents
- Regular monitoring of filtering
- Reporting to relevant Governors meetings
- Attend relevant meeting/committee of Governors

Head teacher and Senior Leaders:

- The head teacher is responsible for the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Head teacher is responsible for ensuring that the E-safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher and Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- SLT will receive regular monitoring reports from the E-Safety Co-ordinator/IT Manager.
- Meets regularly with the E-Safety Governor to discuss issues, review logs and filtering issues Invite and conduct e-safety workshops for parents to increase their awareness of both developments and dangers.
- Liaises with the local authority.
- The Head Teacher and SLT will be aware of the procedures to be followed in the event of serious e-safety allegations being made against a member of staff

E-Safety Co-ordinator

- Has the day to day responsibility for e-safety issues and has a leading role in establishing, monitoring and reviewing the school's e-safety policy.
- Ensure all staff are aware of the e-safety procedures to be followed in the event of an e-safety incident.
- Liaises with the ICT technical staff
- Receives e-safety incident reports and creates a log which will inform future developments.

Designated Safeguarding Lead:

The Child Protection Co-ordinator is aware and trained appropriately in e-safety issues which could relate to child protection issues such as:

- Sharing of personal data
- Access to illegal/inappropriate materials

- Inappropriate online contact with adults and strangers
- Potential or actual incidents of grooming
- Cyber-bullying.

Network Manager/technical staff:

- Ensuring the school's ICT infrastructure is secure and not open to misuse or malicious attack (viral).
- Ensure users use passwords to access the school's networks
- Continue accessing the East Riding Council's preferred internet provider/network manager which filters inappropriate websites.
- ERYCC IT to be informed of issues relating to the filtering problems.
- Keep up to date with e-safety technical information and inform and update others when relevant.
- Complete regular monitoring of network and e-mail use and report any incidents to the E-Safety co-ordinator/Head Teacher/class teacher for further action.
- The administrator passwords for the school's ICT network must be secured and available to the head teacher/ICT Co-ordinator/E-Safety Co-ordinator.
- Maintain an agreed system of access to the school's network by the visiting staff/Trainee teachers (visitor usernames and passwords).

Teaching, Support Staff and visitors:

- Keep up to date e-safety matters and have an understanding of the school's current e-safety policy.
- Read, understood and sign the school's staff acceptable use policy (AUP) (See appendix 4)
- Report any incidents of misuse to the E-safety Coordinator/head teacher/ SLT/ ICT coordinator/class teacher for further action.
- Professionalism must be used when using digital communication (e-mail) and Virtual learning environment (VLE) with the children.
- Personal data is not to be sent electronically unless pupil initials, instead of full names, are used.
- Ensure personal data is not held or viewed on an unprotected computer (passwords, anti-virus, firewalled) and users log out afterwards.
- Digital photographs taken of fully clothed children must be downloaded securely onto the school's server in the appropriate folder (staff shared area/year group) or into the appropriate year group folder in the junior/infant area when appropriate.
- E-safety issues must be embedded in all aspects of the curriculum and other school activities.
- Ensure pupils understand the school's e-safety and acceptable use policy.
- Ensure children have a good understanding of plagiarism and copyright regulations.
- Monitor ICT and extra-curricular lessons.
- Awareness of e-safety issues relating to the use of mobile phones, cameras and handheld devices and follow the current school's policy.
- All staff and visitors will refrain from accessing social media using school equipment.
- All staff and visitors will secure any personal belongings such as mobile phones, cameras etc. in areas away from the children (staff lockers/staff room).

- During educational visits, all staff, volunteers and visitors will only use their personal mobiles in the event of an emergency or when conducting official business.

Pupils:

- Responsible for using the school's equipment and ICT systems appropriately.
- Refrain from accessing social media using school equipment.
- Responsible for the security of their password and must not allow other users access to their user account. They must report any issues of misuse to their class teacher/Computing Subject Leader/head teacher/SLT.
- Have good research skills and avoid plagiarism and copyright issues.
- Awareness of types of abuse on-line and understand the importance of reporting incidents of abuse, misuse and access to inappropriate materials.
- Know the school's policy on mobile phones, cameras and hand held devices.
- Adopt good e-safety practice at all times

Parents/carers:

- Understand the importance of the appropriate and safe ways of using the internet/mobile phones.
- Read parents' newsletters, national leaflets, website information relating to developments/issues in e-safety.
- Accessing the school's website responsibly.
- Development of children's understanding and awareness of risks such as cyber bullying, grooming, sharing and distributing inappropriate images etc. through the promotion of E-Safety Day (E-Safety Assembly and classroom activities).
- Development of children's awareness of the quality, accuracy and relevance of the material/information contained on websites during non/discrete lessons.
- Use of passwords by staff and visitors to prevent misuse.
- All parents/carers and refrain from accessing social media using school equipment.
- All parents/carers will secure any personal belongings such as mobile phones, cameras etc in areas away from the children (staff lockers/staff room).
- During educational visits, all parents/carers and visitors will only use their personal mobiles in the event of an emergency or when conducting official business.

Appendix 1

E-safety Concern Form

Date:

Person completing the form:

Concern identified:

Passed to:

Action taken/Outcome:

Resolved: Yes/No

Further action required: Yes/ No