St Clare's Abbey Primary School

Amor Dei Aliorum Literarumque

The best interests of our children must be a top priority in all our actions - Article 3

Online Safety Policy

Ratified by Board of Governors: June 2016
Review Date: June 2017. Reviewed due to new circulars: February 2017. Reviewed March 2018
Reviewed September 2023

We are a school committed to promoting the rights of our children as per the UNICEF Rights Respecting Schools programme. Our work in this aspect of school life promotes the following articles:

Article 12: Every child has the right to say what they think in all matters affecting them, and to have their views taken seriously.

Article 16: Every child has the right to privacy. The law should protect the child's private, family and home life.

Article 17: Every child has the right to reliable information from the mass media. Television, radio, newspapers and other media should provide information that children can understand. Governments must help protect children from materials that could harm them.

Article 19: Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and mistreatment by their parents or anyone else who looks after them.

Article 28: Every child has the right to an education. Primary education must be free.

Article 29: Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures and the environment.

Article 31: Every child has the right to relax, play and join in a wide range of cultural and artistic activities.

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens".

DENI Online Safety Guidance, Circular number 2013/25

ICT

The term, Information and Communications Technology (ICT) covers a range of resources from traditional computer-based technologies to the fast evolving digital communication technologies.

Some of the Internet-based and electronic communications technologies which children are using, both inside and outside of the classroom, are:

- Websites
- Learning Platforms / Virtual Learning Environments
- Email and Instant Messaging
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting - Skype/Facetime
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- IPads and other tablet devices with internet access
- Smart watches
- Coding devices such as Sphero and drones.

While these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with their use.

Online Safety

This policy operates in conjunction with the following school pastoral policies:

- Policy for Promoting Positive Behaviour,
- Child Protection Policy and

- Anti Bullying Policy.
- Data Protection Policy.

It has been written collaboratively with staff, parents and pupils and ratified by the Board of Governors. Some comments made by these stakeholder groups during consultation meetings were:

"My concern is that they will become part of a world that I know nothing about."

(Parent Representative)

"I worry that I should be teaching my child, not him teaching me."

(Parent Representative)

"I know that everything that is posted online is not true."

(School Council Survey)

"I know that if someone is unkind to me online I can tell someone I trust."

(School Council Survey)

This policy will be reviewed each school year, or sooner if required, as we know that the success of its implementation rests on the level of 'buy in' we have from our whole community.

Rationale

> ***"All schools should have their own Online Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. Online Safety must be built into the delivery of the curriculum. ICT is a compulsory cross curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills"***
>
> *DENI Online Safety Guidance, Circular number 2013/25*

It is the responsibility of the schools, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Online Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. We must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

What we understand by Online Safety

- Online Safety concerns safeguarding children and young people in the digital world.
- Online Safety emphasises learning to understand and use new technologies in a positive way.
- Online Safety is less about restriction and more on education about the risks as well as the benefits so pupils can feel confident online.
- Online Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.
- Online Safety is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

In ***St Clare's Abbey P.S.*** we understand our responsibility to educate pupils in Online Safety. We aim to teach children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Scope of the Policy

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of the School. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure Online Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to Online Safety incidents that occur outside of school hours, the School will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. Online Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of Online Safety incidents outside of the School, will be dealt with in accordance with School Policies.

The school will monitor the impact of the policy using:

- The Online Safety log Book which is stored securely and monitored by the Online Safety Leads and Child Protection Team.
- Monitoring reports on Securus Software
- Reports from Internet Filtering System.
- Surveys/Questionnaires of stakeholders.

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinators to keep abreast of current Online Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Digital Schools 360 degree online safety review and Childnet.

Mrs McParland and Mr Clarke have responsibility for leading and monitoring the implementation of Online Safety throughout the school. The ICT co-ordinators will work closely with the **Designated teacher for Child Protection (Mrs Donnelly)** and **Deputy Designated teachers for Child Protection (Mrs Toner, Miss O'Shea, Mrs Doherty, Mrs Gallagher (nursery), Mr Byrne, Mrs McGoldrick & Mrs Davey)** to promote Online Safety and address any concerns that may arise in this area. Incidents will be recorded in the Online Safety log Book which is stored securely and monitored by the Online Safety Leads, Principal and Child Protection Team.

The Principal/ICT Co-ordinators update Senior Management and Governors with regard to Online Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Principal and Vice Principal

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community. Although the day to day responsibility for online safety will be delegated to the Online Safety Leads (OSLs), all issues arising will be managed with the involvement of the principal and regular monitoring reports will be disseminated by OSLs with principal.
- The Principal and Vice Principal have identified procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal and Vice Principal are responsible for ensuring that the Online Safety Leads and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Vice Principal ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. (Mrs Donnelly meets with Online Safety Leads termly or more often as needed to monitor the effectiveness of the Online Safety Log system. This will include Securus reports. Mrs Monaghan will meet with Todo Tech termly, or more often as needed, to monitor the effectiveness of the iPad filtering system and to plan for further updates.)

ICT Co-Ordinators

The ICT Co-ordinators will lead Online Safety within the school and take day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

The ICT Coordinators will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place. These are recorded in the Online Safety Log Book.
- Provide training and advice for staff.
- Liaise with C2K and school ICT technical staff.
- Liaise with the EA and DENI on Online Safety developments.
- Work with Mrs Donnelly (Safeguarding Team) to receive reports of Online Safety incidents and create a log of incidents to inform future Online Safety developments.
- Meet with Mrs Monaghan, Mrs Donnelly and Safeguarding Team to investigate abuse of social network sites by pupils if necessary.
- Attend relevant meetings with Board of Governors.
- Discuss current issues, review incident logs (where relevant) with Online Safety Group comprising of ICT Coordinators, Mrs Donnelly, Mrs Downey, Mr Doran (BoG) and two Digital Leaders.
- Monitor and report to senior staff any risks to staff of which the Online Safety coordinator is aware
- Oversee the review of the 360 Degree Safe Mark Award awarded in 2017.

Writing and Reviewing the Online Safety Policy

This policy, supported by the school's 'Acceptable Use Agreements' for staff, governors, visitors and pupils and the 'Staff Code of Conduct' is to protect the interests and safety of the whole school community. It is linked to other school policies including those for:

- ICT
- Policy for Promoting Positive Behaviour
- Child Protection
- Anti-bullying.

It has been agreed by the Senior Management Team, Staff, parents and pupils and has been ratified and adopted by the Board of Governors. The Online Safety Policy and its implementation will be reviewed annually.

Roles and Responsibilities

Governors

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 Governors receiving regular information about Online Safety incidents and monitoring reports.

Mr Mark Doran has taken on the role of Online Safety Governor.

He will:

- have meetings with the Online Safety Coordinators and Online Safety Group.
- monitor Online Safety incidents logs
- report to relevant Governors.

Training will be given to the Governors by:

- Attendance at training provided by relevant external agencies/staff in school.
- Participation in school's training/information sessions for staff or parents.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. This group comprises of Mrs Donnelly (CP Team), Mrs McParland and Mr Clarke (Online Safety Leads), Mr Doran (Board of Governors) and two Digital Leaders. The group will also be responsible for regular reporting to the SLT and Board of Governors.

Members of the Online Safety Group will assist the Online Safety Leads with:

- The production / review / monitoring of the school Online Safety Policy / documents.
- Mapping and reviewing the online safety provision – ensuring relevance, breadth and progression.
- Monitoring network / internet / incident logs.
- Consulting stakeholders – including parents / carers and the students / pupils about the online safety provision.
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Safeguarding Team

The Safeguarding team is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data (ref Data Protection Policy revised as per GDPR protocol)
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

The member of the **Safeguarding team** responsible for reporting **Online Safety concerns** to is **Mrs Donnelly**.

The Network Managers

The Network Managers (C2K, Todo Tech, Mrs McParland and Mr Clarke) are responsible for ensuring:

- The school's technical infrastructure is secure and not open to misuse or malicious attack.
- The school meets required online safety technical requirements and any EA Online Safety Policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That the use of the network/internet/learning platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the principal/Online Safety Leads/CP Team for investigation/action/sanction.
- The school Internet access is filtered through the C2k managed service using a Websense filtering solution and via the Classnet system facilitated and monitored by school and Todotech. This system was risk assessed and approved by Governors for installation. The safeguarding reassurances and key guidance documents provided by Todotech personnel are attached to the policy for reference.
- That monitoring systems are implemented and updated as agreed in school policies.

*Websense assesses all websites based on their content and adds them to a category. (Green – available, Red – unavailable) All users are given access to a core group of green sites. The school has the facility to customise security options where need arises. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

Mrs McParland and Mr Clarke, will monitor that C2K Online Safety measures, as recommended by DENI, are working efficiently within the school. IE that:

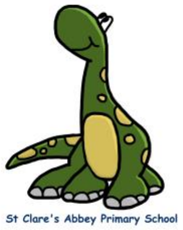
- C2k/Classnet operates with robust filtering and security software.
- Monitoring reports of the use of C2k / Classnet are available on request.
- The school infrastructure and individual workstations are protected by up to date virus software as updated by C2K. (Coordinated updates)
- The school meets required Online Safety technical requirements
- Users may only access the networks and devices through a properly enforced password protection policy ie passwords are regularly changed.
- The filtering policy is applied and that its implementation is not the sole responsibility of any single person.
- They keep 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.

- The "administrator" passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place.

The Role of the Staff

Teachers are the first line of defence in Online Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unacceptable behaviour to illegal activity.

- All staff have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- All staff will read, understand and sign annually the staff AUP.
- All staff will report any suspected misuse or problem to principal/Online Safety leads/CP Team for investigation/action/sanction.
- All staff are responsible for ensuring that all digital communications with pupils, parents, carers should be on a professional level and only carried out using official school systems.
- No filtering service is 100% effective; therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not our approach rather children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Children are taught what Internet use is acceptable and what is not.
- Children are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Children are taught to be Internet Wise. In St Clare's Abbey our Digital Mascot 'Techno' has been created to make our pupils aware of these risks and how to keep themselves safe online. They will be taught Techno's 4 rules of online safety.



<u>Contact</u>
Never talk to strangers online or give them your details.
<u>Content</u>
If unsure always tell and show an adult.
<u>Conduct</u>
Always be kind online no matter what way you contact anyone.
<u>Commercial</u>
Never open any pop-up windows or marketing emails. Always tell an adult.

Pupils

Pupils will

- Be responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- 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.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

"My concern is that they will become part of a world I know nothing about."

(Parent Representative in consultation group)

Parents/carers have an important role to play in promoting Online Safety. We encourage all parents/carers to become involved in Online Safety discussions and activities with their child.

- The school website contains a page dedicated to Online Safety with links to sites such as CEOP's thinkuknow, Childline, and the Kidsmart page which parents can use with their children. The school app and Twitter account will be used for notifications.
- The school communicates relevant Online Safety information through parents' evenings/newsletters, the school website/app and Twitter account.
- Monthly Online Safety newsletter distributed through seesaw and put on the website provides parents with up-to-date, relevant information.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement with their child.
- Parents/carers are required to give written consent to images of their child being taken/used. Updated in line with GDPR.

"I worry that I should be teaching my child, not him teaching me."

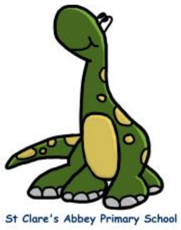
(Parent Representative)

Parents are reminded regularly that it is important to promote Online Safety in the home and to monitor Internet use. The following guidelines are provided- that they should:

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor online time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know Techno's rules and the SMART tips and promote them at home.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Risks and Responses

The Internet is an exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Pupils will be informed that network and Internet use will be monitored.



Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.
A planned online safety program is embedded across the curriculum and lessons are regularly visited .
We have identified **4 Key areas of risk (Contact, Content, Conduct and Commercial)** and have highlighted the steps that we will take to educate and equip our pupils with the skills and knowledge required to minimise the risk and address it should it arise. In St Clare's Abbey our Digital Mascot 'Techno' has been created to make our pupils aware of these risks and how to keep themselves safe online.

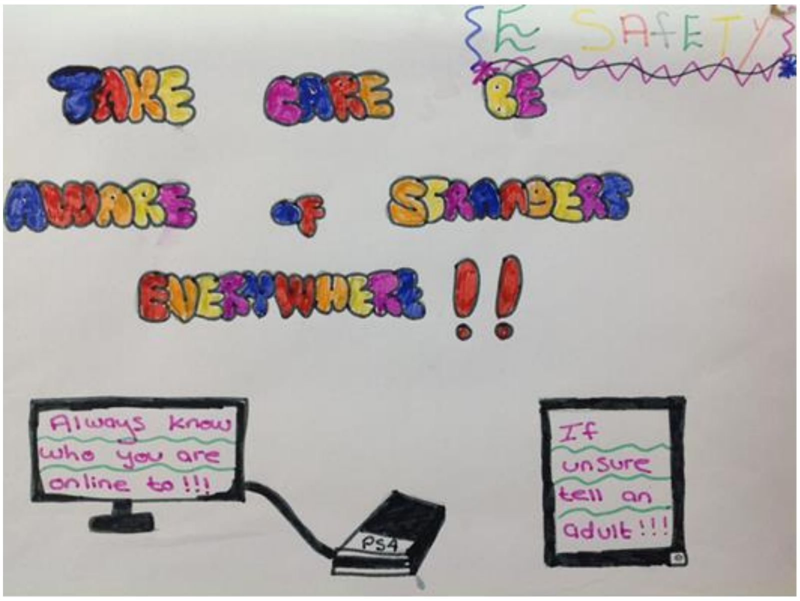
Risk 1: Potential Contact with Strangers

Techno says, "Never talk to strangers online or give them your details."
Children may come into contact with someone online who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons, e.g. grooming.
Personal Information can be accessed leading to unauthorised access to / loss of / sharing of personal information.

To address this risk within St Clare's Abbey our children will be taught:

Never talk to anyone online that you dont know.
Contact
NEVER talk to strangers online or give them your details.

- **That people are not always who they say they are.**
- **That "Stranger Danger" applies to the people they encounter through the Internet.**
- **That they should never give out personal details.**
- **That they should never meet alone anyone contacted via the Internet, and**
- **That once they publish information (e.g. send inappropriate photographs) it can be disseminated with ease and cannot be destroyed.**


E SAFETY
TAKE CARE BE
AWARE of STRANGERS
EVERYWHERE !!
Always know who you are online to!!!
PS4
If unsure tell an adult!!!

<u>**Cyber-bullying**</u>. We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites.

Having surveyed the School Council we discovered that a small number of children had been subjected to cyber bullying outside of school. CEOP data states that 21% of 8 – 11 year olds have been deliberately targeted, threatened or humiliated by an individual or group through the use of mobile phone or the internet (Beatbullying, Virtual Violence ll).

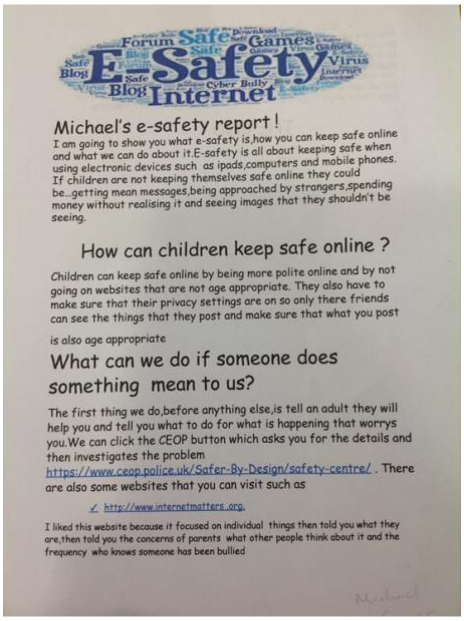
If it takes place, cyber-bullying will be dealt with in line with the school's Anti-bullying Policy, Policy for Promoting Positive Behaviour and other Pastoral Procedures and Practices.

To reduce this risk, within St Clare's Abbey pupils will be taught:

- **That if they feel they are being bullied by e-mail, through social networking sites, gaming sites/platform, text or online and that they cannot get it to stop through their own efforts that they should always tell someone they trust.**
- **Not to reply to bullying, threatening text messages or e-mails as this could make things worse.**
- **Not to send or forward abusive texts or e-mails or images to anyone.**

- **That whilst they may be able to appear anonymous most messages can be traced back to their creator and cyber bullying can constitute a criminal offence.**
- **To keep abusive messages as evidence.**

By: Anna Mc Peter
P.5
Be Good Not Bad
Yay
sniff
you're real nice
when I grow up I want to be just like you !!
don't make others Sad
you're so stuPiD
I NEVER want to See you again because you're too DUMB


Forum Safe Games Blog E-Safety Virus Internet Cyber Bully

Michael's e-safety report!

I am going to show you what e-safety is,how you can keep safe online and what we can do about it.E-safety is all about keeping safe when using electronic devices such as ipads,computers and mobile phones. If children are not keeping themselves safe online they could be...getting mean messages,being approached by strangers,spending money without realising it and seeing images that they shouldn't be seeing.

How can children keep safe online ?

Children can keep safe online by being more polite online and by not going on websites that are not age appropriate. They also have to make sure that their privacy settings are on so only there friends can see the things that they post and make sure that what you post is also age appropriate

What can we do if someone does something mean to us?

The first thing we do,before anything else,is tell an adult they will help you and tell you what to do for what is happening that worrys you.We can click the CEOP button which asks you for the details and then investigates the problem https://www.ceop.police.uk/Safer-By-Design/safety-centre/ . There are also some websites that you can visit such as

✓ http://www.internetmatters.org.

I liked this website because it focused on individual things then told you what they are,then told you the concerns of parents what other people think about it and the frequency who knows someone has been bullied

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school

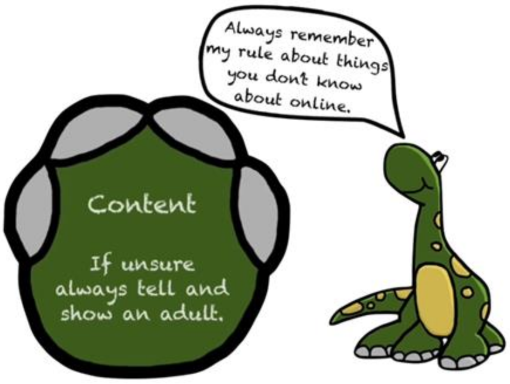
We will keep records of reported cyber-bullying incidents in the Online Safety Log Book to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations; support and sanctions (see Anti Bullying Policy).

Risk 2: Accessing Inappropriate Content

Techno says, "If unsure always tell and show an adult".

"I know that everything that is posted online is not true."

(School Council Survey)


Always remember my rule about things you don't know about online.
Content
If unsure always tell and show an adult.

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Children can access illegal, harmful or inappropriate images or other content.

Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

There is access to unsuitable video / internet games.

There is an inability to evaluate the quality, accuracy and relevance of information on the Internet. Materials may contain misleading and inaccurate information e.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

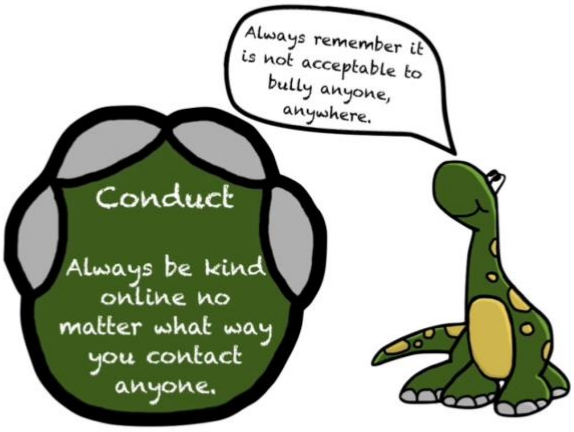
To address this risk within St Clare's Abbey our children will be taught:

- **That information on the Internet is not always accurate or true. In KS2 they use the Rule of 3 - see the same 'fact' from three different reliable sources.**
- **To question the source of information.**
- **How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.**

Risk 3: Online Behaviour and Conduct

Techno says, "Always be kind online no matter what way you contact anyone."

- There is potential for excessive use of technologies, and the internet, which may impact on social and emotional development and learning of our pupils (too much screen time).
- It is tempting for pupils to 'Copy and paste' information from the


Always remember it is not acceptable to bully anyone, anywhere.
Conduct
Always be kind online no matter what way you contact anyone.

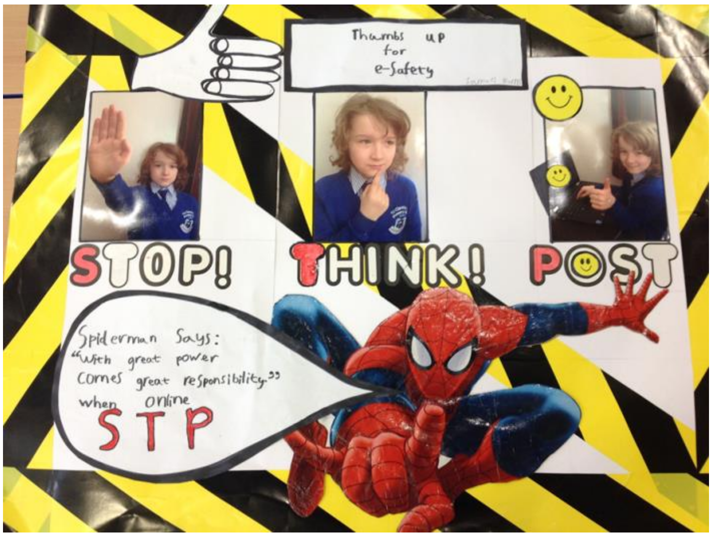
internet without referencing it or fully understanding what they are reading.

- There is the possibility that children could illegally download music, videos and games.
- Unintentional sharing and distribution of personal images without an individual's consent or knowledge.
- The potential for 'negative' online behaviours which may impact on future opportunities.

To address this risk in St Clare's Abbey children will be taught:

- Excessive hours spent on the Internet/gaming is not healthy.
- In all relevant lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.
- The dangers and possible repercussions of downloading illegally.
- It is illegal to take pictures of anyone without them knowing.
- Nothing they send, write or do on the internet can ever be erased completely.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential through good educational provision to build children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to deal with these risks.


Thumbs up for e-Safety
STOP! THINK! POST
Spiderman Says: "With great power comes great responsibility." when online STP

<u>Risk 4: Commercial</u>

Techno says, "Never open any pop-up windows or marketing emails. Always tell an adult."

When using the internet children may encounter commercial advertising pop-ups or be asked to click on links that may be harmful to them or the computer.

To address this risk within St Clare's Abbey our children will be taught:

Always remember my rule about commercial advertising online.
Commercial
Never open any pop up windows or marketing emails. Always tell an adult.

- **Adverts on the internet should always be questioned.**
- **Not to click on or open any pop-ups.**
- **Always tell an adult.**

Whilst no scheme of work is in place for the teaching of Online Safety, we address it constantly through:

- Technosaur 'Techno' (Launched 20th January 2017). Techno has four eSafety rules (Digital Paw Print). These correspond to the four risks outlined above. Techno's rules will be built on as pupils progress from P1 – P4 and reinforced and extended from P5 – P7. P1 – Content, P2 – Conduct, P3 – Contact, P4 – Commercial.
- Providing opportunities across the curriculum for children to develop their Online Safety skills.
- Educating children on the dangers of technologies that may be encountered outside school when opportunities arise (either at designated times or as incidental contexts arise).

BE Safe... online
Conduct
Content
Commercial
Contact
If unsure always tell and show an adult
UNITE FOR A BETTER INTERNET
Techno
Techno wants You to be safe on all devices!!
UNITE FOR A BETTER INTERNET
TECHNO'S SAFETY MESSAGE
STAYING SAFE ONLINE
BE CAREFUL:
Who you speak to
What information you share
Of your privacy settings
AND REMEMBER:
If you see something online that makes you feel uncomfortable, unsafe or worried tell a trusted adult IMMEDIATELY!!!
PICCOLLAGE

Education – Parents/Carers

Many parents and carers have only 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers.

Education and Training – Staff and Volunteers

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

- Regular updating of the Online Safety policy and any Online Safety issues are shared with staff annually and intermittently as policy changes. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out in the course of each three-year school development cycle (refer to current self-evaluation document for details).
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Leads (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations (refer to staff in service schedule for details).
- The Online Safety Leads provide advice, guidance and training to individuals as required using CEOP.

Training - Governors

Governors regularly take part in training on Child Protection issues including online safety training. This is delivered digitally in school by centrally provided resources (all governors involved) and at training conferences led by the Education Authority (key governors i.e. lead governor for Child Protection, Online Safety Governor and Chairperson).

Technical Infrastructure/Equipment, Filtering and Monitoring.

The school will be responsible for ensuring that the school 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:
A more detailed Filtering Policy can be found in the appendix.

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements – C2k & 'Todo' technical support.

- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password by C2K Managers who keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and are required to change their password every term. FS children also use Simplified Login provided by C2K Managers.
- The "administrator" passwords for the school ICT systems, used by the Network Manager are also be available to the Principal and kept in a secure place (email).
- To minimise the need for removable media (e.g. memory sticks / CDs / DVDs) staff are asked to use a school laptop/Surface Pro for work at home so that data held securely on their documents or staff folders will be used via password protected/ secure C2 K downloads. Encrypted USB pens will be provided for instances when this approach is not possible.** Updated practice from May 25th 2018 with the implementation of GDPR.
- We are aware that Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy in the appendix for further detail).

Online Safety implications for online conduct for Staff

- Staff will be aware that Internet use can be monitored and traced to the individual. **Professional conduct is essential.**
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- They have read, understood and signed the school's Staff Acceptable Use Policy.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know to **report an incident of concern to the school Designated Teacher for Child Protection/Safeguarding Team and/or the teachers responsible for Online Safety**.
- New staff members receive information on the school's Online Safety Policy and Acceptable Use Agreement as part of their induction.
- All teachers are encouraged to ensure Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- St Clare's Abbey staff review each year as part of this policy's review the level of internet filtering allocated to each group of users.

- Staff are asked not to use home email accounts for school business. Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School's Code of Conduct – professional conduct is essential.
- School staff will not add children as 'friends' if they use social networking sites. They will not correspond with parents or relatives of pupils about school business via social networking sites. Staff will not discuss school business via these sites.
- Staff will ensure that pupils have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998(KS2).
- Staff monitor ICT activity in lessons, extracurricular and extended school activities.
- Staff are aware of Online Safety issues related to the use of mobile phones, camera and hand-held devices and monitor their use and implement current school policies with regard to these devices.
- Staff will undertake all Online Safety training as organised by the school.

NB Please refer to the 'Staff Code of Conduct' policy, written and adopted in Term 1 of 2014/15 school year - opening year of St Clare's Abbey and updated most recently in 2017.

Online Safety implications re specific aspects of ICT

Password Security

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password. They are encouraged to keep details of usernames and passwords private.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

E-mail:

- Pupils may only use C2k e-mail/school provided Gmail accounts on the school system and at home for submission of homework e.g. Office 365.
- 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.
- Forwarding chain letters is forbidden.
- Sending or displaying insulting or offensive messages/pictures is forbidden.

- Using obscene language is forbidden.

Social Networking:

- Through the C2k system our school currently blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff will not add children as 'Friends' on social networking sites.

Portable Technologies

- The use of portable devices such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.

Mobile Phones

- Pupils are not allowed to bring personal mobile phones to school unless required to do so by class teacher as part of their learning e.g. to be used with Google Cardboard, to be used for Leavers' Celebration. In **exceptional circumstances** a pupil will be allowed to have their mobile phone in school when permission is sought in writing from the Principal. The phone must be kept in their school bag and switched off during the day. It must not be switched on while on school grounds. Phones are brought into school at own risk.
- Staff should not use personal mobile phones for personal reasons during working hours. If there is a need to be contactable please inform Mrs Donnelly or Mrs Monaghan and this can be accommodated.

Given the vastness of our building and its grounds the following exceptions will be made:

  - All teachers are asked to keep their phone on when outdoors to facilitate contact with school office.
  - The First Aides are asked to keep their phones switched on in the event of an emergency.
  - The school caretakers are also asked to keep their phones switched on.

- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity unless number is blocked (at staff's discretion). Staff will have the use of a school phone where contact with pupils or parents is required.

Smart Watches

- Pupils are not permitted to wear smart watches with camera/video capabilities.

iPads

iPads are used for digital storytelling, internet research, and to support learning and teaching across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet Wise and apply the Internet safety rules. They will not be allowed to use iPads to:

- Take photos of pupils/staff without permission or direction from the teacher.
- Take videos of pupils/staff without permission or direction from the teacher.
- Communicate through any app unless using their own name e.g. Minecraft.

Managing Video-conferencing

- Videoconferencing will be via the C2k network/Classnet to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Digital Recordings

- We record learning and teaching on occasions as a tool to share best teaching practice, celebrate pupil achievement and enhance home/school partnerships. We gain permission to use these from child and parent and adhere to GDPR guidelines to ensure that our practice is fully compliant.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission, except where disclosed to the Police as part of a criminal investigation.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. See Data Protection Policy.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs/videos of pupils are published on the school and third party websites. This consent form is considered valid for the entire school year unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the School Website/ App, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents. Signed consent will be sought.

Authorising Internet Access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's Online Safety rules. These Online Safety rules will also be displayed clearly in all rooms.
- All parents/guardians will be asked **annually** to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's Online Safety rules and within the constraints detailed in the school's Online Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Handling Online Safety Complaints or Misuse

- Complaints of Internet misuse will be dealt with by a senior member of staff. If deemed necessary PSNI education partners may become involved.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the Online Safety incident logbook (kept securely in the main office).

- As part of the Acceptable Use Agreement children will know that if they deliberately break the rules they could be stopped from using the Internet/E-mail and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Complaints regarding cyberbullying will be dealt with in line with the school Anti-Bullying Policy.
- Pupils and parents will be informed of the complaints' procedure.
- Any complaint about staff misuse must be referred to the Principal and governors.

Communicating the Policy:

With pupils:

- Online Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week/Online Safety Week.

Staff:

- All staff will be involved in discussions regarding Online Safety and will have access to a copy of the Online Safety Policy.

Parents:

- A parents' working group inputted into this policy.
- The policy is displayed on the website / App and all parents are notified of this.
- At the start of each year parents receive a copy of the Code of Conduct and are asked to sign the Acceptable Use Agreement on behalf of their child.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinators.

This policy is the governors' responsibility (day to day management given to principal) and they will review its effectiveness annually. They will do this through liaison with the ICT Co-ordinators and a representative of the Safeguarding Team.

We sought guidance from 'Todo tech' in compiling this policy.

St Clare's Abbey Primary School

Amor Dei Aliorum Literarumque

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

In St Clare's Abbey our Digital Mascot 'Techno' has been created to make our pupils aware of online risks and how to keep themselves safe. Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Monaghan.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂ -

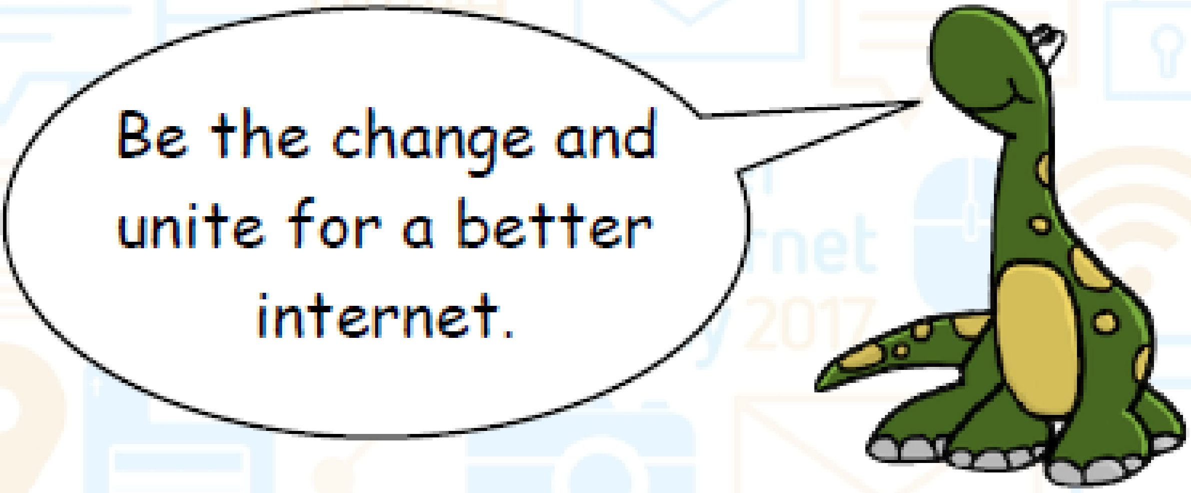
Parent/ carer signature
We have discussed this document with ……………………………………………(child's name) and we agree to follow the Online Safety rules and to support the safe use of ICT at St Clare's Abbey Primary School.

Parent/ Carer Signature ………………………………………………….

Class …………………………………. Date ………………………………

Primary Pupil Acceptable Use
Agreement / Online Safety Rules

- I will only use ICT in school for school purposes.
- I will not take a personal mobile device into school.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible as per Techno's rules.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately as per Techno's rules.
- I will not give out my own/others details such as name, phone number or home address as per Techno's rules. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not take a photo or make a recording without permission of the person/persons involved.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will only open e-mail attachments from people I know, or who my teacher has approved.



Techno's E-Safety Rules

Content

If you are not sure always show and tell an adult.

Contact

Never talk to strangers online or give them your details.

Conduct

Always be kind online.

Commercial

Never open any pop-up windows or marketing emails. Always tell an adult.

Follow these SMART TIPS to Stay Safe Online

S

Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

M

Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

A

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

R

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

T

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet. Produced by: Northern Area Child Protection Committee.

Code of Practice

For Primary Parents regarding Online Safety rules.

- I will give written confirmation to the school to allow my child(ren) access to the Internet through a filtered service.
- I will keep computer/laptop/tablet devices in a communal area of the home.
- I will monitor online time and be aware of excessive hours spent on the Internet/gaming.
- I will take an interest in what the children are doing. I will discuss with the children what they are seeing and using on the Internet/gaming.
- I will remind them that their online reputation can last a lifetime and so they should always be responsible, polite and sensible whilst online.
- I will read Techno's Rules and the SMART tips, and discuss these regularly with my child.
- I will discuss the fact that there are websites which are unsuitable.
- I will discuss how children should respond to unsuitable materials or requests.
- I will remind children never to give out personal information on the Internet.
- I will make my child aware that people online may not be who they say they are.
- I will ensure that my child(ren) know(knows not to arrange to meet someone they meet online.
- I will talk to my child about safety when using the Internet in places other than home or school.
- I will be aware that when pupils use the C2K online learning environment 'MySchool' whether in school or outside school, that they will be agreeing to certain terms and conditions of appropriate usage, these terms are available to view by clicking on the 'Acceptable Use Policy' at the bottom left of their MySchool home page.
- When taking photographs of my child in school performances etc they will be for private usage and will not be uploaded onto any social media sites.

Useful Websites

- Think u know - https://www.thinkuknow.co.uk/
- Kidsmart - http://www.kidsmart.org.uk/
- Webwise - http://www.webwise.ie/sphe/
- Ceop - https://www.ceop.police.uk/safety-centre/
- Childline - https://www.childline.org.uk/Pages/Home.aspx
- Childnet - http://www.childnet.com/young-people/primary

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Monaghan.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be via password protected downloads onto a secure school laptop or encrypted, eg memory stick.
- I will not install any hardware or software without permission of Mrs Monaghan.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- I will support and promote the school's Online Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ____ Date ____________

Full Name ____ (printed)

Job title __________________________________