



St Charles' RCVA Primary School

e–Safety Policy

School Mission Statement

The community of St. Charles School believes that Jesus is at the heart of everything that we do. We are committed to giving every child every opportunity to achieve their potential in mind and body in a happy, safe and caring environment.

Why does St Charles' School need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

As a school, we must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. We must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

We must be aware of our legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the DCC e–Safety Policy and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors
- Our school has formed an e-safety committee
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

The School e-Safety Coordinator is Mrs. B. Hill

Policy approved by Head Teacher: J. A. Reeves Date: September 2015

Policy approved by Governing Body: Mr. C. Butler (Chair of Governors)

Date: October 2015

The date for the next policy review is September 2016

Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- St. Charles has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with DCC and DfE;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- St. Charles Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- St. Charles School will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

The following statements require adaptation according to the pupils' age:

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to use search engines appropriately for their age.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including DCC and network suppliers.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- St. Charles School will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office. www.ico.gov.uk advice is available from www.ico.gov.uk/for_organisations/sector_guides/education.aspx
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- St./ Charles has a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

St. Charles has created an excellent website and has effective communication channels, which inspire pupils to publish work of a high standard. St. Charles websites celebrates pupils' work, promotes the school and publishes resources for projects.

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

Images of a pupil should not be published without the parent's or carer's written permission. Pupils also need to be taught the reasons for caution in publishing personal information and images online.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- St. Charles School will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

It is important to establish a protocol for establishing the responsibility for checking a site which needs changes to the filtering.

- If a contentious website is requested (e.g. youtube) it will be discussed by the e-safety committee.

- For other sites the responsibility for checking the suitability of the site rests with the teacher requesting access.
- St. Charles School's broadband access includes filtering.
- St. Charles School has a system in place to make changes to the filter, including deciding who is responsible for authorising changes.
- The school works with DCC to review filtering
- The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or CEOP

How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.

Systems include complex standalone equipment and software based systems such as Skype.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information will not be put on the school Website.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

How are emerging technologies managed?

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy. (Pupil Mobile phones will be kept securely by the class teacher during school hours)

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

St./ Charles School has information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

For advice and guidance relating to a contravention of the Act, contact Lawrence Serewicz:
lawrence.serewicz@durham.gov

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

St. Charles School will allocate Internet access to staff and pupils on the basis of educational need. In a primary school, where pupil usage should be fully supervised, all pupils in a class could be authorised as a group.

- St. Charles School will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

How will risks be assessed?

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the fact that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system.

- St. Charles School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor DCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- St. Charles School will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Durham Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used.

e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Child Protection Coordinator.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- St. Charles School will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Durham.

How will e-Safety complaints be handled?

Parents, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. e-Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e-Safety Coordinator. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Durham Police Safer Schools Partnership Coordinator responsible for the school or the Children's Safeguard Team.

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

- St. Charles School will liaise with local organisations to establish a common approach to e-Safety.
- St. Charles School will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: <http://www.digizen.org/cyberbullying>

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- St. Charles School will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
 - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
 - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
 - Parent/carers of pupils will be informed.
 - The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms be managed?

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave St. Charles their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
 - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
 - b) The material will be removed by the site administrator if the user does not comply.
 - c) Access to the LP for the user may be suspended.
 - d) The user will need to discuss the issues with a member of SLT before reinstatement.
 - e) A pupil's parent/carer may be informed.

How will mobile phones and personal devices be managed?

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
 - Their use can render pupils or staff subject to cyberbullying;
 - Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
 - They can undermine classroom discipline as they can be used on “silent” mode;
 - Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.
-
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
 - Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
 - Pupils’ mobile phones and personal devices are not permitted to be used within the school site and should be given to the class teacher to securely keep until the end of the school day.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to ‘silent’ mode, Bluetooth communication should be “hidden” or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

Many pupils are very familiar with culture of mobile and Internet use and it is wise to involve them in designing the School e–Safety Policy, possibly through a student council. As pupils' perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

Consideration must be given as to the curriculum place for teaching e–Safety. This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever pupils are using the internet.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
 - Childnet: www.childnet.com
 - Kidsmart: www.kidsmart.org.uk
 - Orange Education: www.orange.co.uk/education
 - Safe: www.safesocialnetworking.org
-
- All users will be informed that network and Internet use will be monitored.
 - An e–Safety training programme is established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
 - Pupil instruction regarding responsible and safe use will precede Internet access.
 - An e–Safety module is included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
 - e–Safety training is part of the transition programme across the Key Stages and when moving between establishments.
 - e–Safety rules or copies of the student Acceptable Use Policy is posted in all rooms with Internet access.
 - Safe and responsible use of the Internet and technology is reinforced across the curriculum and subject areas.
 - Particular attention to e–Safety education is given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods.

Staff are given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse for DCC employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. School must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, St. Charles School will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, is provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents’ support be enlisted?

Internet use in pupils’ homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child’s use elsewhere in the community is covered by an appropriate use policy.

- Parents’ attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it’s implications with their children.

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: <http://clickcleverclicksafe.direct.gov.uk>

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Durham EDS – E-safety, Teaching and learning advice Tel: 0191 3834370

Durham Safeguarding Children Board (DLSCB): www.durham-lscb.gov.uk

ICT Service Desk – Changes to filtering Tel: 03000 261100

ICTSS Service Desk – All other ICT issues Tel: 01388 424999

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent e-Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety

Kidsmart: www.kidsmart.org.uk

Schools e-Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: <http://en.teachtoday.eu>

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com