ST ALBAN’S CATHOLIC PRIMARY SCHOOL

Christ Be Our Light

INTERNET USE & E-SAFETY POLICY

Autumn 2020

This Policy will be reviewed in Autumn 2021

The internet can be used to encourage the gathering, sharing, communicating and collaboration of information. It is very powerful in motivating and engaging children and offers means of communicating beyond the school. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. Alongside the educational benefits lie significant risks.

Benefits of the Internet to Education

- Access to worldwide educational resources
- Educational and cultural exchanges between pupils worldwide
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Access to experts in many fields; for pupils and staff

Use the internet to enhance learning

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location and retrieval
- Pupils will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy
- Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work

Some of the dangers pupils may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development of the learner

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

St Alban’s Catholic Primary School is committed to a comprehensive E-safety agenda in order to monitor, manage, reduce and minimize risk where ever possible. Our aim is that children engage confidently with a range of online materials where this supports their learning and that they develop knowledge of how to manage the associated risks effectively.

This e-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. It should be read in conjunction with the Acceptable Use Policies for pupils, staff and parents.

Consultation

Consultation with whole school community has taken place through the following:

- Staff meetings
- School / Student / Pupil Council
- Governors meeting / sub committee meeting
- School website newsletters

Monitoring

The school will monitor the impact of the e-safety policy through incident reporting logs, internet activity through the proxy server, internal network usage. Pupils, parents and staff will review their understanding through regular auditing.

Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents /carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and responsibilities

E-safety Coordinator **(FLOWER)**
There will be a named member of staff who is responsible for managing e-safety in school. The e-safety co-ordinator will :

-Lead the e-safety committee.
-Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies/documents.
-Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
-Provide training and advice for staff.
-Liaise with the Education ICT Service who check overall aspect of school e-safety.
-Liaise with school ICT technical staff.
-Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
-Respond appropriately to any e-safety incidents ensuring the safety of the pupil concerned.
-Meet regularly with the E-Safety Governor to discuss current issues.
-Review incident logs and filter/change control logs.
-Attend relevant meeting/committee of Governors.
-Reporting regularly to Senior Leadership Team._

Governing Body

There will be a named link Governor who will attendance e-safety training provided by the Local Authority/ National Governors Association/ Cambridgeshire Education ICT Service or other relevant organisation and participate in school training/information sessions for staff. They will consulted upon and approve any policy changes.

Users of network/online resources

Each user must take responsibility for his or her use of the computer network and Internet. If a pupil accesses an offensive or harmful site by mistake, the pupil must close the device and report what has happened to a member of staff immediately. Similarly, if a pupil notices another pupil has accessed such a site, they must also report it to a member of staff. These responsibilities are clearly stated in the school's ICT Code of Conduct which is shared by all pupils at the beginning of each school year and revisited by teachers as necessary.

Network Management

The school's ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Cambridgeshire Education ICT Service Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance .There will be regular reviews and audits of the safety and security of school ICT systems. Servers, wireless systems and cabling will be securely located and physical access restricted.

Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee. All users will be provided with a username and password of their classes by the ICT Support Officer who will keep an up to date record of users and their usernames.. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Users will be required to change their password in the event that it is shared or compromised.

Filtering

We maintain a single point of access to the Internet through a central connection to the County's Internet Service, which is EastNet. Their Internet filtering system is maintained to block material that is inappropriate for children. Items filtered include obscene visual images, child pornography and material that is harmful to minors. It must be noted, however, that due to the nature of the Internet no filtering system is 100% perfect. In response to this, we can ask the County's Internet Service to block additional sites we deem are unsuitable and also ask them to unblock sites we feel are appropriate.

Monitoring

Children are only allowed to access the Internet when supervised by a teacher or other member of staff. The teacher or staff member supervising the pupil has the primary responsibility of monitoring the pupil's safe and appropriate use of the Internet. Education ICT Service provides a monitoring system that records the Internet sites accessed. Parents who do not wish their children to use the Internet at school should notify the school in writing.

Live Web Searches

Staff may use Google to carry live web searches with children. Children are not allowed to live web searches without supervision by a teacher or other member of staff.

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line.

Messaging

Messaging includes posting text, participating in discussion groups. Children are allowed to use messaging in CLASSDOJO within the class between the teacher and other pupils when this work is part of a school project or directed by the teacher. Children may also be invited to use communication tools on CLASSDOJO. All other forms of messaging are prohibited at school.

Email accounts

Staff use of personal email is prohibited and subject to the school's disciplinary procedures. Unregulated communication can put individual members of staff and the school at risk of prosecution. School business includes but is not limited to communication with pupils, parents, governors, other members of staff and third parties such as suppliers of school equipment or government agencies. For this reason auto-forwarding of email to external accounts is prohibited and staff must make themselves aware of the risks posed by forwarding any mail externally. As a school, we advise that when communicating with the children via email, staff use the CLASSDOJO account which is transparent for monitoring.

CLASSDOJO- link to their policy

New and Emergent Internet Uses

Emerging technologies will be reviewed for the education value and a risk assessment will be undertaken before use in school is allowed. Commercially produced CDs etc. may be used as a teaching resource providing they have been reviewed and checked by a member of staff first.

Security

We use the County's Internet Network, EastNet, which provides a secure network for the school community.

Confidentiality of Information

Personal information concerning pupils will not be disclosed or used in any way on the school website without the specific permission of a parent or guardian. Pupils are not permitted to provide private or confidential information about themselves or others on the Internet.

The point of contact on the Website will be the school address, school email and telephone number. Staff or pupil's home information will not be published. Pupils' work published on the web will not be identified by their surnames. Including photographs of groups of pupils on the school website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school. Such photographs will only be used for educational purposes and the identity of children will be protected. The full name of a pupil will never be included alongside the photograph. Parents who do not wish their child's photograph to be used on the school website should notify the school office in writing.

Copyright

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained. At an appropriate age, pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Home Use & Advice for parents

Children will be encouraged to use the internet at home where this support their learning. The school will endeavour to keep parents informed of developments in e-safety through regular newsletter bulletins, the passing of information through email and where appropriate with parents meetings. Advice will be made available where appropriate. General recommendations for Internet use by pupils at home are contained in Appendix A.

Appendix A

When using the Internet:

- Children should never reveal personal information such as their name, home address or phone number or any information that might allow someone to locate them.
- Children should never agree to meet a person face-to-face whom they have "met" on the Internet without their parent's permission and without an adult being present.
- If someone attempts to arrange a meeting with a child through the Internet, the child must report this communication to their parent or guardian.
- Instant messaging should not be used by children at home unless explicitly approved and supervised by parents.
- Children should choose screen names carefully (e.g. Soccer_Kicks is better than Pretty_Sally13).
- Children should never telephone an online 'acquaintance' without parental permission, because caller ID can trace a phone number and from that information, the child's address can be found.
- Nobody should reply to harassing, threatening or sexual messages but should report any such communication immediately to the police.

Filtering at home

There are a number of filtering programs that allow parents to block sites and monitor their child's use of the Internet, including the time of day, number of hours and types of access (such as chat, web, or newsgroup activities). It is recommended that parents use this type of filtering if their child will be using the Internet without direct parental supervision. Filtering can be set to restrict all Internet use when parents are not home.
For more information refer to:
http://www.childnet-int.org/
http://www.getnetwise.org/
http://www.safekids.com/

Search engines, such as Google, should be used with extreme caution as the potential for unsuitable sites to be listed is relatively high. At school, the children use http://search.bbc.co.uk/ If using Google for web searches, click on the Preferences button and set your search preferences to Strict Filtering.

Location of Computers in the Home

It is recommended that parents place computers used by children in a heavy traffic area of the home. The best place for a home computer used by a child is in an area such as the living room or kitchen. The worst place is a child's bedroom.

Parent / Child Dialogue

It is recommended that parents:

- Have constant dialogue with their child about what they are doing online
- Encourage their child to show them what they are doing
- Consider establishing a "Code for Internet Use" for the home

Violations

The Internet has much value in today's world and is available in many public places including our libraries. If a child violates the home "Code of Internet Use", it is recommended that parents try to use the situation as an occasion for learning in the first instance, rather than immediately "pulling the plug" on all home Internet access.

Reporting

It is imperative that any illegal or suspicious contact with a child on the Internet is reported to the police immediately.

Online Safety Advice

- Think U Know
- Parental Control Settings
- NSPCC Online Safety
- Internet Matters