St Edward's Catholic First School
Parsonage Lane, Windsor SL4 5EN
Head Teacher: Mrs Sarah Matthews
Telephone: 01753 860607
Fax: 01753 869107
office@secfs.org.uk
www.stedwardscatholicfirstschool.co.uk

E-SAFETY POLICY

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

The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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.

Ethos

It is the duty of the School to ensure that every child and young person in its care is safe. Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support e-Safe practices in school `and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

E-safety is a partnership concern and is not limited to school premises and equipment or the school day. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the School's Anti-Bullying and Behaviour Policy. Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about e-safety incidents and monitoring reports.

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

- The Head teacher is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Head teacher will be responsible for applying sanctions that may include:

- interview/counselling by an appropriate member of staff
- informing parents/carers
- removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system.
- referral to the police.

E-Safety Coordinator / Officer:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with the Local Authority / relevant Board;
- liaises with school technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- attends relevant meeting of Governors if required;
- reports regularly to Senior Leadership Team.

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;

- that the use of the network is monitored in order that any misuse / attempted misuse can be escalated for investigation / action / sanction;
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy (AUP);
- they report any suspected misuse or problem to the head teacher for investigation / action / sanction;
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the e-safety and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection / Safeguarding Designated Person is trained in e-safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- will 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 cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play the primary role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to social media, parents' sections of the website and school endorsed on-line activity that may contain recorded pupil data.

Reviewed:	Head Teacher	February 2019
Approved:	Curriculum Committee	18th March 2019
Ratified:	FGB	18th March 2019
Review frequency	Annually	