St Dunstan's Catholic Primary School
E-Safety Policy

"As we grow with God, we learn from each other."

New technologies bring new opportunities but they also bring unfamiliar challenges and risks. The purpose of this policy is to ensure that all staff, parents, children and governors understand and agree the school's approach to e-safety.

1. Introduction

1.1 Young people have access to the Internet from many places; home, school, friend's homes, libraries and in many cases mobile devices. Our school has a number of services to help ensure that curriculum use is safe and appropriate, however access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people and parents learn to become safe on-line whilst in school and at home.

1.2 It is neither appropriate to try to eliminate all risks nor possible to do so: learning to deal with risk is an inherent part of a child's development. The aim of this e-safety policy is to ensure that the level of risk is not unacceptably high, and to empower staff, parents and children to identify concerns and to manage the risks. This takes into account each child's strengths, vulnerabilities and stage of development.

2. Internet

2.1 The purpose of Internet access at St Dunstan's School is to support and develop educational standards, support the professional work of the staff and to enhance the school's management information and administration systems.

2.2 Access to the Internet is a necessary tool for staff and students. It helps prepare children for the future and personal development needs. It is a requirement of the National Curriculum for Computing and is implemented across the curriculum.

2.3 Internet access is provided and filtered by Bishop Challoner Catholic Collage and is designed for pupils and staff. Bishop Challoner Catholic Collage has strong filtering systems in place that are age and content appropriate for pupils.

2.4 Internet access is planned to support, develop and extend learning activities.

2.5 Access levels are reviewed to reflect the current curriculum.

2.6 Staff will select sites which support the learning outcomes planned for the pupils' age and maturity.

2.7 Pupils are given clear objectives for Internet use and sign an Internet agreement.

2.8 Pupils are taught how to take responsibility for their own Internet access during lessons.

3. Email

3.1 Pupils may only use the approved email accounts given to them on the school system. Children are not allowed to access personal email accounts or chat rooms whilst in school.

4. Information System Security

4.1 The security of the schools information systems will be reviewed regularly.
4.2 Virus protection will be installed and updated regularly.
4.3 The school uses broadband with firewall and filters.

5. School Website

5.1 The ICT coordinator, Head teacher and Deputy Head teacher will take overall editorial responsibility for content on the school website and ensure it is accurate and appropriate.

6. Publishing pupils images and work

6.1 Written permission from parents or carers will be obtained at the start of the academic year before photographs of pupils are published on the school website. All photographs will be carefully selected and will not enable pupils to be clearly identified, i.e. their picture with their full name.
6.2 Pupil's full names will not be displayed anywhere on the school website.

7. Social Networking and Personal Publishing

7.1 Social networking sites will be blocked unless a specific use is approved.
7.2 Pupils are advised never to give out personal details of any kind which may identify them or their location.
7.3 Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils as the popular social networking sites have a minimum age of 13.

8. Managing Filtering

8.1 The school works in partnership with Bishop Challoner Catholic Collage to ensure filtering systems are as effective as possible.
8.2 If staff or pupils discover unsuitable sites, the school Forensic software will automatically capture a screen shot of that site and it will be automatically sent to the Head Teacher where they will determine action required.

9. Emerging Technologies

9.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

10. Authorising internet access

10.1 The school will keep an up to date record of all staff and pupils who are granted Internet access.
10.2 All staff must read and sign the ICT Acceptable Use Policy.
10.3 Parents and pupils will be asked to sign and return a consent form agreeing to comply with the schools Acceptable Use Policy.

11. Evaluating Risks

11.1 The school will take all reasonable precautions to ensure that users only access appropriate material. However, due to the world wide scale and linked nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school iPad or computer. The school cannot accept any liability for the material accessed, or any consequences of Internet access.
11.2 Any concerns related to E-Safety will be logged on My Concern, which will be reviewed by the DSL and any actions required in response to this will be discussed and organised.
11.3The Head teacher and the ICT coordinator will ensure the E-safety Policy is implemented and compliance with the policy is monitored.
11.4 The school will work towards the '360 degree safe' certificate which involves a thorough review of policies and practice related to digital technology.

12. E-Safety Reporting Systems and Sanctions

12.1 Any E-safety issues or complaints, involving children must be recorded on My Concern.
12.2 Users will have an awareness of how to report issues online, including to CEOP.
12.2 Sanctions are in place for any e-safety abuse or misuse and parents will be informed as relevant.
12.3 Any complaint of a child protection nature must be dealt with in accordance to the school's child protection procedures.

13. Communication of the E-Safety Policy and Raising awareness

13.1 SMART rules for Internet access will be displayed in each classroom.
13.2 Pupil will be informed that Internet use will be monitored.
13.3 Advice on E-Safety will be introduced at an age-appropriate level to raise awareness about the importance of safe, responsible and confident use of electronic media. Children need to be aware of:

- How to avoid, recognise and report inappropriate content
- The need for caution when putting personal information on the web, including an understanding of what personal information is; address, school, email address, phone number etc.
- The need to think carefully before putting any information or pictures online.

13.4 All staff will be given the E-Safety policy and its importance explained.
13.5Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
13.6 Staff will support the efforts of parents to safeguard the welfare of their children.

14. Further Guidance and Support

- www.ceop.gov.uk

The Child Exploitation and Online Protection Centre (CEOP) - brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse.

- www.thinkuknow.co.uk
  This is a website for young people full of information about staying safe online. It includes areas with practical guidance for parents and carers, and for teachers and trainers.
- www.childnet-int.org
  Childnet International is an organisation which works with partners around the world to try to ensure that children and young people are protected from the dangers of the Internet.
- http://www.education.gov.uk/ukccis/about
  The UK Council for Child Internet Safety (UKCCIS) - this site includes information about the Byron Reviews "Safer Children in a Digital World"
- www.virtualglobaltaskforce.com
  The Virtual Global Taskforce is an international alliance of law enforcement agencies working together to make the Internet a safer place.
- www.education.gov.uk/schools/pupilsupport/behaviour/bullying
  This site includes advice for schools on preventing and responding to bullying.
- www.iwf.org.uk
  The Internet Watch Foundation is an organisation which works with the Police and Internet Service Providers to trace those responsible for putting harmful or illegal material on the web.
- www.stopitnow.org.uk
- www.lscbbirmingham.org.uk
  Birmingham Safeguarding Children Board

15. Conclusions

This policy was written in September 2014 by the ICT coordinator. It was last reviewed in January 2020 and will be reviewed again in 2021.