

# ST CATHERINE'S CATHOLIC HIGH SCHOOL



## **E-SAFETY POLICY**

(To be read in conjunction with  
Student and Staff Acceptable Use Policies)

Last Reviewed: January 2012

Review Date: September 2013

St Catherine's Catholic High School in partnership with the whole school community aims to provide an education which reflects the life, values and teachings of Jesus Christ, within the moral, spiritual and doctrinal tradition of the Catholic Church.

In line with the Mission Statement the E-safety policy of the school will endeavour to:

- Give the whole school community the opportunity to develop their potential spiritually, academically and socially
- Ensure provision of equal opportunity by developing a curriculum which caters for the needs of all members of the school community
- Offer a curriculum based on effective teaching which is equally concerned with Christian values as it is with knowledge and skills
- Encourage all members of the school community to respect and value themselves and others
- Encourage relationships which, at all levels of the school community are based on respect, love and forgiveness.
- Work to develop a sense of responsibility for and awareness of the needs of others through all members of the school community
- Create a safe, caring, challenging and enjoyable environment where Students will be helped towards readiness for the opportunities and responsibilities of adult life.

The E-safety policy reflects the Every Child Matters agenda and is underpinned by the Catholic teaching (see appendices). This policy has been written to allow all students to be cherished for who they are, as much as for what they achieve, and to allow all achievement to be recognised and celebrated - Department for Education (DfE).

### **Background Rationale**

The use of new innovative tools in school and at home has been shown to raise educational standards and promote student/student achievement.

The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information
- Risk of being subject to grooming by those with whom they make contact on the internet
- 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
- 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 and learning of the young person

Many of these risks reflect situations in the off line world and it is essential that this E-safety policy is used in conjunction with other school policies (eg Behaviour, Anti-Bullying, Child Protection).

It is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with those risks.

### **Reviewing this Policy**

This policy was written by the E-safety co-ordinator. Consultation with the ICT Working Party, Senior Leadership Team (SLT), Business Manager, Governors, Staff and Parents/carers will also take place. The policy will be reviewed annually by the ICT Working Party and any changes identified reported to the SLT, Business Manager, Governors and staff.

The school will monitor the impact of the policy through:

1. Surveys with students, staff and parents/carers
2. Monitoring logs of students internet activity

### **Who does this policy apply to?**

This policy is relevant to all members of the school community who have access to and use school ICT systems both in and out of school.

### **Roles and Responsibilities**

#### **The Governors are responsible for:**

- Approving the E-safety policy and reviewing the effectiveness of the policy. *It is suggested that a member of the Governing Body takes on the role of E-safety and meets with the E-safety co-ordinator regularly to discuss E-safety matters.*

#### **The Headteacher/SLT is responsible for:**

- Ensuring the safety of all members of the school community.
- Ensuring adequate Continuing Professional Development is provided on issues concerning E-safety within the school
- Following procedures in the event of a serious E-safety allegation being made against or concerning a member of staff or student within the school.

#### **The E-safety co-ordinator/Officer is responsible for:**

- Ensure E-safety is a standing item on the ICT group agenda
- Take a lead role in day to day E-safety issues
- Annually review the E-safety policy of the school
- Provide training within the school community on E-safety
- Meet with the Governor responsible for safeguarding on a termly basis
- Liaise with the Local Authority
- Liaise with the School's ICT Network staff
- Log all E-safety incidents to help inform for future E-safety practices/developments

- Attend relevant meetings where appropriate
- Report regularly to SLT

**The Network Manager/staff are responsible for:**

- Ensuring the school's infrastructure is secure and not open to misuse/attack
- The school meeting the E-safety technical requirements as required
- Remaining at the forefront of E-safety technical information and inform/update others as necessary
- Ensuring data is held in line with the Data Protection Act 1998

**The teaching/support staff are responsible for:**

- Having an up to date awareness of E-safety matters and the school policy
- Implementing the Acceptable Use Policy for staff at the school
- Reporting any suspected misuse/problem to the E-safety coordinator for investigation/action/sanction
- Ensuring all digital communication (email, mobile phone text etc) with students is on a professional level and carried out using only school systems
- When using ICT rooms they reiterate to students the school E-safety policy/acceptable use policy and where there are breaches report through the relevant procedures.
- Ensuring that copyright law is abided by when using materials from the internet
- Ensuring that the virus protection on their school laptop is updated weekly.

**The Child Protection Officer is responsible for:**

- Having an up to date awareness of E-safety matters
- Having an up to date awareness of the potential risk for serious child protection issues such as:
  - Sharing of personal data
  - Access to illegal/inappropriate materials
  - Inappropriate contacts with strangers
  - Potential/actual grooming
  - Cyber-bullying

**The students are responsible for:**

- Ensuring they use school ICT systems appropriately following the school E-safety policy/acceptable use policy.
- Understanding how to report issues of abuse/misuse within school and know how to do so.
- Knowing and following school policy on the use of mobile phones, digital cameras as well as the use of images appropriately.
- Understanding the importance of good E-safety practice when using digital technology both in and out of school
- Ensure copyright is abided by when using information from the internet

## The parents/carers are responsible for:

- Ensuring their child understands the issues surrounding E-safety
- Endorsing the student acceptable use policy. **Please note students will not be given access to the school network until the acceptable use policy has been returned signed by both the student and parent/carer.**

## Teaching and Learning

The purpose of the internet tool in school is to raise educational standards, promote Student achievement, support the professional work of staff and enhance school management functions.

Students at St Catherine's are encouraged to use the internet both within and outside of school to support their learning. It is important therefore to teach them the skills of using it appropriately, knowing and understanding the risks to allow them to take care of their own security.

By allowing students and staff to use the internet we are opening up a vast resource of materials to support their learning and continuing professional development

The school internet access is designed expressly for student use and will include appropriate filtering for the age of Students. St Catherine's maintains a current record of all staff and students who are granted access on the computer network. Both staff and students must sign the acceptable use policy before being allowed access to the school internet agreeing to comply with the E-safety rules. Parents/carers will also be asked to sign a consent form for Student access.

Students will be taught what acceptable use of the ICT facilities is and given clear objectives for internet use. They will be made fully aware of the consequences of breaching these rules.

The school and individual will ensure that copyright law is abided by when materials from the internet are used.

St Catherine's will block all access to social networking sites for all students and staff. Training will be provided to ensure all students are aware of the importance of not providing personal information that would allow another person to identify them/their location. Advice will be given to students on acceptable practice when using social networking sites outside of school. Staff **must not** allow students to access them personally through social networking sites.

The school will work with the relevant agencies to ensure that the systems to protect Students are reviewed and improved. If staff/students discover unsuitable sites these need to be reported to the Network Manager/E-safety co-ordinator.

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

## Managing Information Systems

The security of the school information systems will be reviewed regularly and virus protection will be updated regularly on the school system. Any data that is to be sent over the internet will be sent encrypted.

Any files on the school network will be checked regularly for security purposes. Unapproved files of executables will not be allowed in student areas. Portable media may be used in the school but only following a virus check to ensure they are not infected.

The school will take all reasonable precautions to ensure that users access only appropriate material. Due to the nature of the internet, it is not possible to guarantee access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or consequences resulting from internet use.

The use of the school network without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Personal data held on the school network will be recorded, processed, transferred and made available according to the Data Protection Act of 1998

### **E-mail Accounts**

Students will only be able to use approved email accounts. Should a student receive an inappropriate email they should report it through the Virtual Learning Environment (VLE) misuse facility immediately. In any email communication students should not reveal personal information about themselves or arrange to meet a person unless they know the person. Access to external email accounts in school will be blocked.

All staff will have access to a school email account which will allow them to communicate with people outside of school. It is up to the member of staff to ensure that all communication regarding school is done so in a professional manner and using only school systems, this includes the use of windows messenger.

### **The school VLE/website**

The contact details on the website should be the schools address, phone number/fax number and email address. Staff/students personal information must not be published. The Headteacher is responsible for ensuring that all information on the school website is appropriate.

Written permission should be kept up to date and gained annually from all parents/carers before any images of students are placed on any communication for the school for that academic year (This includes newsletters, letter, website etc).

### **How to report an E-safety incident**

Complaints of internet misuse will be dealt with by the E-safety co-ordinator. These can be reported personally by completing the misuse proforma or through the misuse facility on the VLE. Any complaint about staff misuse must be reported directly to the Headteacher.

Students, parents/carers and staff will all be informed of the complaints procedure. It is expected that both students and parents/carers will work to support the school should any issue arise.

Consequences to students that will be implemented by St Catherine's in the cases of misuse will include:

- Detention with Form Tutor
- Detention with Head of year
- Detention with Member of SLT
- Parents/Carers being informed / invited into school to discuss the situation
- Removal of internet access for a given period
- Removal of network access for a given period
- School exclusion for fixed period

Consequences to staff will be at the discretion of the Head teacher.

## **Communicating E-safety**

### **Students**

All ICT rooms will contain posters about E-safety and acceptable use of the internet and school computer network. Students will be informed that their network and internet activity is monitored. E-safety will be taught through PSHCE and ICT lessons. Internet Safety week will be on the school calendar each year and assemblies for all year groups will take place during this time to promote E-safety.

### **Staff**

All staff will be given the E-safety policy and its application and importance explained. Training on E-safety will be provided on a cycle annually.

### **Parents/Carers**

Parents/carers will receive information regarding E-safety through school newsletters, information sheets and a dedicated page on the school website. A partnership approach with parents/carers is to be encouraged with a display being made available throughout the year on E-safety at all events. Parents/carers will be invited to a meeting to be held once per year to provide information on the latest developments on E-safety.

### **Acknowledgements**

Trevor Harris; Calderdale LA; E-safety Policy Draft March 2009

KCC Children Families and Education Directorate, April 2007; Schools E-safety Policy Guidance

Bishops Conference Document "Common Good in Education" 1997

Chris Devanney; Diocese of Leeds

Signed: Mrs P Sheard (Head)      Signed: Mr T Miskell (Chair of Governors)

Date ratified by Governing Body: January 2012

Date to be reviewed: September 2013

