



# St Augustine of Canterbury Catholic High School

## **E-Safety Policy**

**This policy complies with the Equality Act 2010 and has been fully Equality Impact Assessed.**

### **Equality statement**

The governors and staff are committed to providing the full range of opportunities for all students, regardless of gender, disability, ethnicity, social, cultural or religious background. All students have access to the curriculum, and the right to a learning environment, which dispels ignorance, prejudice or stereotyping.

### **Rationale**

In our digital age, it is important that we educate all of our stakeholders about e-Safety. First and foremost, it should be remembered that e-safety is a safety issue and not an IT and computing issue. It is part of the wider safeguarding agenda in schools. For example, cyber bullying is considered alongside real-world bullying.

### **Purpose**

- To empower students to take responsibility for staying safe online.
- To equip parents/carers with the skills to ensure e-safety in and out of the home environment.
- To provide staff with the skills and knowledge to both teach and be aware of e-Safety issues.
- To ensure that students are safe online; that they know and understand how to stay safe online.
- To ensure that roles and responsibilities are clearly defined and adhered to.

### **Roles and Responsibilities**

All staff are responsible for e-safety at St Augustine's. However, the e-Safety Co-ordinators at St Augustine's are Mr Bennett and Mr Cubbin. The named governor for Safeguarding in the school is Mr Cubbin.

### **Learning and Teaching**

#### **Why the internet and digital communications are important**

- The internet is an essential element in 21<sup>st</sup> Century life for education, business and social interaction. St Augustine's has a duty to provide students and staff with high-quality internet access as part of the learning experience.
- Internet use is part of the statutory curriculum and a necessary learning tool for staff and students.

#### **The Benefits of the internet and digital communications for education**

- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.

- Vocational, social and leisure use in libraries, clubs and at home.
- Professional development for colleagues through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administrative data.
- Access to learning every day of the year and at any time of the day.

### **Internet use will enhance and extend learning**

- The school internet access was designed expressly for student use and includes an appropriate filtering system (see Agilisys).
- Clear boundaries have been set for appropriate use of the internet and digital communications and have been discussed with staff and students (L&T group, E-Safety and IT group, student forums, staff meetings and INSET, cross curriculum dimensions).
- Students will be educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation (see Computing and whole school curriculum).
- Staff will guide students in online activities that will support the learning outcomes planned for the students.

### **Students will be taught how to evaluate internet content**

- The school will ensure that the use of internet derived materials by staff and by students complies with copyright law (see copyright procedures).
- Students will be taught to view critically the materials they read and show how to validate information before accepting its accuracy especially when considering such things as radicalisation and extremism (see Computing curriculum, all staff).
- Students will be taught to acknowledge the source of information used and to respect the copyright when using internet material in their own work (see Computing curriculum, all staff).
- Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example, to close the page and report the incident immediately to the member of staff.
- If students (or staff) discover unsuitable sites, the URL (web address), time, date, and content will be reported to a senior member of staff or the Child Protection Officer (Mr Cubbin).

### **Managing Information Services and Internet Access**

#### **Security**

- The security of the school information services will be reviewed regularly (see Agilisys Managed Service Agreement).
- Virus protection (Sophos) and Firewall (Windows Firewall) will be installed and updated regularly.
- Portable media may not be used without specific permission and a virus check, including USB pens/sticks (see AUP policies).
- Unapproved system utilities and executable files will not be allowed in school either in students' work areas, attached to e-mail or on any other portable media.
- Files held on the school's network will be regularly checked.
- The Securus software system will be monitored by Mr Bennett in conjunction with Mr Cubbin, House Managers and the Headteacher, Mr Hagan.

## E-mail

- Students and staff must only use approved e-mail accounts on the school system.
- Students must immediately tell a member of staff if they receive offensive e-mail.
- Students and staff must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission (see AUP policies).
- Use of words included in the Websense 'banned' list will be detected, logged and acted upon through the pastoral system.
- Access in school to external, personal e-mail accounts may be blocked.
- Excessive social e-mail use by students can interfere with learning and may be restricted.
- The forwarding of chain letters is not permitted.
- Students and staff are expected to adhere to the following network etiquette (for further details, see the *E-mailing Parents'* document):

<ul style="list-style-type: none"><li>• Be polite</li></ul>	<ul style="list-style-type: none"><li>• Illegal activities are strictly forbidden</li></ul>
<ul style="list-style-type: none"><li>• Use appropriate language</li></ul>	<ul style="list-style-type: none"><li>• Note that e-mail is not guaranteed to be private</li></ul>
<ul style="list-style-type: none"><li>• Do not reveal the personal address, phone number or other personal details of yourself or other users</li></ul>	<ul style="list-style-type: none"><li>• System administrators have access to all mail</li></ul>
<ul style="list-style-type: none"><li>• Do not get abusive in your messages to others</li></ul>	<ul style="list-style-type: none"><li>• Messages relating to or in support of illegal activities may be reported to the authorities</li></ul>
<ul style="list-style-type: none"><li>• Do not use the network in such a way that would disrupt the use of the network by other users</li></ul>	<ul style="list-style-type: none"><li>• Do not take part in activities that can be related to radicalisation or extremism.</li></ul>

## Published content on the school website

- The website address is [www.staug.org.uk](http://www.staug.org.uk)
- Staff or student contact information will not be published. The only contact details will be the school address, e-mail and telephone number.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing students' images and work

- Photographs that include students must be selected carefully so that individual students cannot be identified or their image misused.
- Student's full names will not be used anywhere on the website or in any online space when in association with photographs.
- Most parents' have given permission when signing the AUP policy for photographs of their children to be used for publicity purposes, including the school's website. Please note however, that some parents have not given permission and a list of these students is available from the Office Manager.
- Students' work can only be published with the permission of the student and parents/carers.

## Social networking and personal publishing

- Social networking sites will be blocked unless a specific use is approved by the Headteacher.
- Students and staff are advised never to give out personal details of any kind which may identify them or their location.

- Students and staff are advised not to place personal photographs on any school social networking space. On a personal level outside of school, if staff/students use social media sites they are advised to consider how public their information is and it is recommended using the highest privacy settings possible.
- Students and staff are advised about security and are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others. Staff should not accept students or parents/carers as 'friends' or 'followers'.
- Students and staff are advised not to publish specific and detailed private thoughts.
- Students and staff are informed that bullying can take place through social networking especially when a space has been created without a password and others are invited to see the bully's comments.
- St Augustine's has a Facebook page used to communicate directly with parents/cares – the reply option has been blocked. The school also has a Twitter feed to keep stakeholders up to date with news and information.
- St Augustine's currently uses Twitter and/or Instagram as a means of learning and communication (see above).

### **Managing Filtering**

- St Augustine's works in partnership with St Helens LA and Agilisys (IT Managed Service since 2011) to ensure that filtering systems are as effective as possible.
- If staff or students discover unsuitable sites, the URL, time and date must be reported to the IT Technicians using the online reporting system and/or E-Safety Co-ordinator.
- The IT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal will be reported to the police.

### **Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Student mobile phones will not be allowed in school.
- Staff will be issued with the school mobile phone for trips and visits.

### **Protecting Personal Data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All staff have a legal duty to protect the privacy of information relating to individuals.

### **Policy decisions**

#### **Authorising internet access**

- The school will maintain a current record of all staff and students who are granted internet access.
- All users, students and staff, must read, sign and abide by the Acceptable Use Policy before using any school ICT resource.
- Parents/carers will be asked to sign and return a consent form for student access at the Year 6 Parents' Information and Induction Evening.

#### **Risk Assessment**

- St Augustine's will take all reasonable precautions to ensure that users access only appropriate material. However, the school does not accept liability for material accessed, or any consequences of internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.

### **E-safety complaints procedure**

- Complaints of student internet misuse will be dealt with through the pastoral system.
- Mr Bennett will check the 'captured views' section of Securus on a daily basis during term time and report any misuse to the appropriate member of staff, depending on the seriousness of the incident.
- Parents/carers and students will need to work in partnership with staff to resolve issues.
- Sanctions within the school behaviour policy include: interview/counselling by the House Manager; informing parents or carers; detentions; removal of internet or computer access for an agreed period of time.
- Any complaint about staff misuse must be referred to the Headteacher.

### **Communications Policy**

#### **Introducing the policy to students**

- Rules for internet access will be posted in all networked rooms.
- Students will be informed that internet use will be monitored.
- Units of work on responsible internet use will be included in the PSHEC and Computing programmes of study covering both school and home use. However, this is the responsibility of all staff (see E-Safety Curriculum Plan).
- Students will actively participate in the annual Internet Safety Day each February.

#### **Introducing the policy to staff**

- All staff will be given the school e-safety policy through the Staff Handbook.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff development in safe and responsible internet use and on the school e-safety policy will be provided as required.

#### **Enlisting the support of parents/carers**

- Parents'/carers' attention will be drawn to e-safety issues through newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively to inform parents/carers without alarm.
- Using a triangular method of communication between staff, parent/carer and student, a partnership will be encouraged. This will include parent's events with demonstrations and suggestions for safer home internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents/carers.

### **E-safety contacts and references**

#### **Child Exploitation and Online Protection Centre**

[www.ceop.gov.uk](http://www.ceop.gov.uk)

**Think u know**

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Kidsmart**

[www.kidsmart.org.uk](http://www.kidsmart.org.uk)

**Childline**

[www.childline.org.uk](http://www.childline.org.uk)

**UK Safer Internet**

[www.uksaferinternetcentre.org.uk](http://www.uksaferinternetcentre.org.uk)

## **References**

St Hilda's High School, Kent  
St Benedict's Catholic High School, Kent  
BECTA

## **Summary**

It is clear that as a community, we all have a key role to play in e-safety. This policy will be reviewed annually through the student and staff ICT/E-safety groups and should be read in conjunction with the *Staff Handbook and Staff Computing and ICT Handbook*.

**Reviewed on: May 2017**

**Next Review Date: May 2018**

**Reviewed by: ..... (Signature)**

## Equality Impact Assessment

**Title of Policy, Decision, Practice or Programme:** E-Safety

**Department:** Computing and ICT

**Responsible Officer:** Paul Bennett

**Date Completed:** May 2017

**Date Review Required:** May 2018

1. **Aims:** Please identify the main aims of the policy, decision or function?

**To empower students to take responsibility for their safety online**

2. **Impact upon different sections of the School / Community / Staff Groups:**  
It is essential that policies, decisions, practices and programmes advance equality of opportunity and foster good relations within the community, and do not leave the School vulnerable to discrimination claims.

Equality Strand	Issue	How will this be taken into account?
General Issues	No issues	
Age	No issues	
Disability – Including Carers	No issues	
Sex (Gender)	No issues	
Transgender	No issues	
Race (Ethnicity)	No issues	
Pregnancy and maternity	No issues	
Religion or Belief	No issues	
Sexual Orientation	No issues	
Community Cohesion	No issues	

### 3. Indirect discrimination

**Are there any rules or requirements in the policy / decision that:**

- a Can be met by a considerably smaller proportion of people from a particular section of the community?
- b Is to the disadvantage of that group?
- c Cannot be justified by the aims and importance of the policy?

If all three conditions apply then there may be evidence of indirect discrimination.

No

### 4. Publishing the results of the assessment:

**Decisions** This Equality Impact Assessment Report must be used to inform the Decision. Attach the Equality Impact Assessment Report as an appendix in the Decision documentation.

**Policy** This Equality Impact Assessment Report must be used to inform Policy development. Attach the Equality Impact Assessment Report as an appendix in the published Policy.

**Practices and Programmes** The Equality Impact Assessment Report must be used to inform Practice and Programme development. Attach the Equality Impact Assessment Report as an appendix in the Practice or Programme documentation.