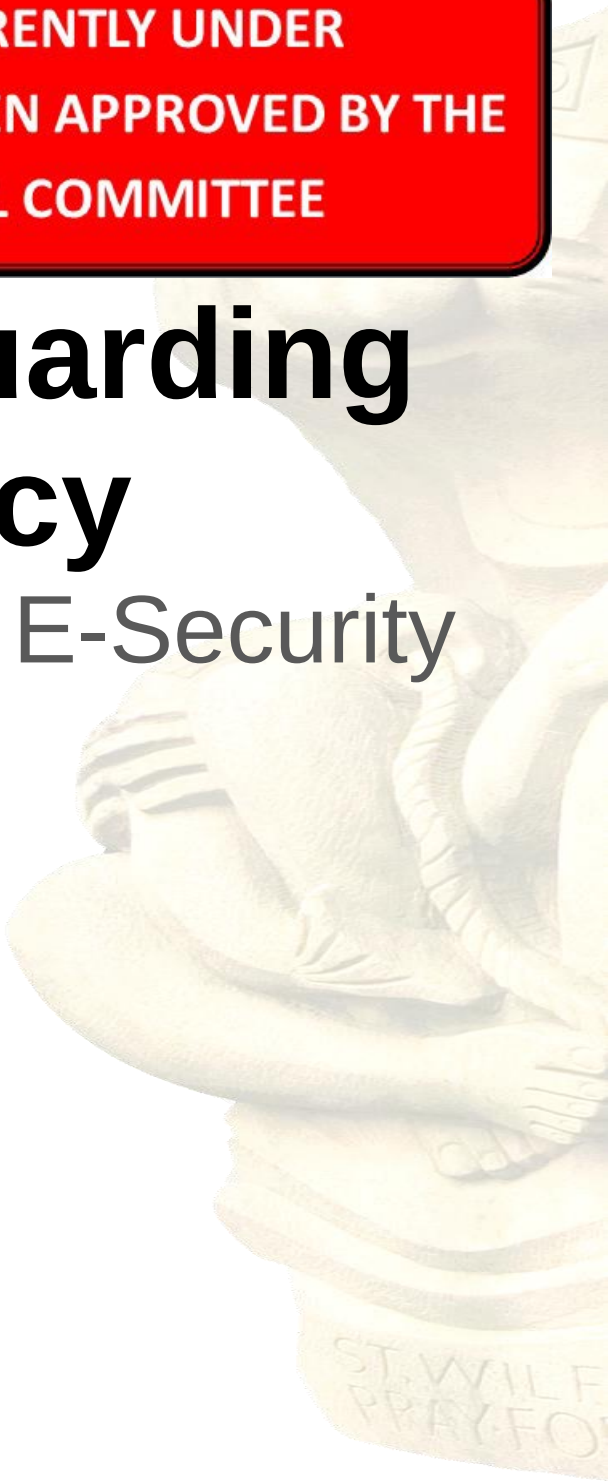
St. Wilfrid's

Catholic High School & Sixth Form College, a Voluntary Academy

THIS POLICY IS CURRENTLY UNDER REVIEW AND HAS NOT BEEN APPROVED BY THE ACADEMY COUNCIL COMMITTEE

E-Safeguarding Policy

E-Safety and E-Security



Keeping the Faith in Education

Contents

POLICY DOCUMENT	**E Safeguarding Policy 2016**
Legislation: Education/Other	Recommended document for Academy Schools
Lead Member of Staff	Headteacher
Lead Governor	
Revision Date	July 2017
Date last Reviewed	July 2016
Governor Committee	GOV/HT
Review Frequency	1 year
Publication date:	July 2016
Chair of Governing Body signature:	
Date:	

Rational

The internet and other digital and information technologies are vehicles for a wide range of opportunities for both staff and students at St Wilfrid's. Electronic communication has become a regular teaching tool and can promote stimulating and effective learning. The staff and students of St Wilfrid's should have an entitlement to safe internet access at all times.

The requirement to ensure that staff and students are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in the educational setting from the Headteacher and governors to the senior leaders, classroom teachers, support staff, parents, members of the community and the students themselves.
Although the use of these exciting and innovative tools in school has creative opportunities for advancement 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
- 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 and learning of the young person.

It is very difficult to remove all these risks completely. It is therefore essential, through training and educational provision to make staff and students aware of the risks to which they may be exposed, so that they are informed and skilled to manage any potential risk, if it were to occur. At St Wilfrid's we wish to ensure that we have an educational culture within the school to encourage responsible and positive usage of the internet.

St Wilfrid's must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by:

- Headteacher / Senior Leaders
- ICT Technical staff
- Governors

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

- Staff meetings
- School / Student / Pupil Council
- INSET Day
- Governors meeting / sub committee meeting
- Parent Evenings
- School website / newsletters

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires with students, teachers and parents and carers
- Students use in lessons
- Staff feedback from CPD

Who is the Policy for?

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 out of school, but is linked to membership of the school.

The school will inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Governors receiving regular information about e-safety incidents and monitoring reports will carry this out.

- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors committee

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.

- The Senior Leadership team will receive regular reports from the BART team regarding known incidents of internet misuse.
- The Headteacher and 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. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant HR / disciplinary procedures)

The Pastoral Deputy Headteacher with responsibility for Child Protection and Safeguarding:

…should be trained in e-safety issues and be aware of the potential for serious child protection 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

The Pastoral Deputy Headteacher with responsibility for Child Protection and Safeguarding:

- 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 having taken place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reports regularly to the Headteacher

The IT Manager and IT Support Staff:

…are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are encouraged to be changed regularly
- appropriate and effective filtering is in place
- that he / she keeps 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, Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator 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 school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Pastoral Deputy Headteacher for investigation / action / sanction
- digital communications with students (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students 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

Students:

- …are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they have to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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
- Students should know who to speak to in order to raise the alarm over any e-safety issue.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children are. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns and literature. St Wilfrid's provides their own seminars for parents where appropriate. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- Accessing the school website / VLE / on-line student records in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision are expected to sign a similar AUP as above before being provided with access to school systems.

Policy Statements

Education – students

The education of students at St Wilfrid's in e-safety is an essential part of the school's e-safety provision. Students need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education is provided in the following ways:

- e-safety lessons are provided as part of ICT and Computing lessons and the PSCHE programme. This should cover both the use of ICT and new technologies in school and outside school
- Important e-safety messages are be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Guidelines and information specifically for students are accessible on the school website

The most important lesson is that students should know whom to speak to if they see or hear about any potential e-safety issue that they feel uneasy about or are unhappy with. Those people are: Mrs H Gilroy (the Headteacher), Mr A Lewis (Deputy Headteacher in charge of Pastoral issues), and Mrs M. James (leading safeguarding professional).

Education – Parents and Carers

Parents and carers have an essential role in the education of their children in the use of new technologies and in the monitoring / regulation of the children's on-line experiences. Parents may underestimate how often students and young people come across potentially harmful and inappropriate material on the internet and may be unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, parents have a specific website e-safety section
- E-Safety training is offered and provided by school on-site and advertised extensively
- Guidelines and information specifically for parents are accessible on the school website

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of e-safety training is made available to staff via the CPD provision.
- IT support staff will receive regular updates through bulletins and training sessions and review guidance documents.
- Guidelines and information specifically for staff are accessible on the school website

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by relevant organisations
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Manager (or other person) and will be reviewed, at least annually.
- All users will be provided with a username and password by the IT helpdesk who will keep an up to date record of users and their usernames. Users will be encouraged to change their password regularly.
- The "administrator" passwords for the school ICT system, used by the ICT Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Users will be made responsible for the security of their own username and password; they 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.
- The school will maintain an effective filtering service that will be reviewed regularly
- In the event of the IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- The Network Manager will consider requests from staff for sites to be removed from the filtered list. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual/potential e-safety incident to the IT Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts, which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data should not be sent over the internet or taken off the school site unless safely encrypted, or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students 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.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the students visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (and other relevant person) can 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.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998, which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password-protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (note: many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communication Technologies

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening, or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used for identification and communication with members of staff.

Useful website for staff

www.childnet.com.

Childnet has an international mission to work in partnership with others around the world to help make the internet a safe place for children.
Childnet works in three main areas of Access, Awareness, Protection, and Policy.

1. **Access**, helping children and young people to use the internet constructively
2. **Awareness,** helping children and young people acquire new 'net literacy' skills and giving advice to industry, organisations, parents, teachers, and carers about the internet and mobile safety.
3. **Protection and Policy**, working with others to help protect children from being exploited in the online environments provided by new technologies as well as seeking to initiate and respond to policy changes

Much of the general e-safeguarding information and guidance in this policy is from two sources:

An internet provider, Yorkshire & Humberside Grid for Learning (YHGfL),
http://www.yhgfl.net/eSafeguarding …who have comprehensive guidelines and resources for e-safety including audit tools.

'E-Safety Support' https://www.e-safetysupport.com …who are a division of Kodo Education

St Wilfrid's Catholic High School and Sixth Form College: A Voluntary Academy
Student ICT Acceptable Use Agreement

- I will use ICT systems in school, including the internet, email, digital video, and mobile technologies only for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken with the permission of those involved and stored and used for school purposes in line with school policy. Images will not be distributed outside of the school network.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Dear Parent/ Carer

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of E-Safety and know how to stay safe when using any ICT. A copy of this E-Safety and Data Security Policy can be found on the school web site. Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or E-Safety coordinator.

We have discussed this document and …….. (student name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at the School.

Parent/ Carer Signature: ……

Student Signature: ……

Form: …… Date ……