St Richard's Catholic College

E-Safety Policy

The Policy was approved by the Governing Body: **March 2016**

Chair of Governors:_____

The Governing Body will review the policy in March 2017

Contents

1. Introduction
2. Scope of the Policy
3. Policy Statements
    - 3.1 Education – Pupils
    - 3.2 Education – parents / carers
    - 3.3 Education & Training – Staff
    - 3.4 Curriculum
    - 3.5 Technical – infrastructure / equipment, filtering and monitoring
    - 3.6 Use of digital and video images - Photographic, Video
    - 3.7 Responding to Incidents of misuse
    - 3.8 School Filtering Policy
    - 3.9 Communications
    - 3.10 Data Protection
4. Legislation
    - 4.1 Computer Misuse Act 1990
    - 4.2 Data Protection Act 1998
    - 4.3 Freedom of Information Act 2000
    - 4.4 Communications Act 2003
    - 4.5 Malicious Communications Act 1988
    - 4.6 Regulation of Investigatory Powers Act 2000
    - 4.7 Trade Marks Act 1994
    - 4.8 Copyright, Designs and Patents Act 1988
    - 4.9 Telecommunications Act 1984
    - 4.10 Criminal Justice & Public Order Act 1994
    - 4.11 Racial and Religious Hatred Act 2006
    - 4.12 Protection from Harassment Act 1997
    - 4.13 Protection of Children Act 1978
    - 4.14 Sexual Offences Act 2003
    - 4.15 Public Order Act 1986
    - 4.16 Obscene Publications Act 1959 and 1964
    - 4.17 Human Rights Act 1998
    - 4.18 The Education and Inspections Act 2006
5. Links to other organisations or documents
6. Resources

1. Introduction

At St Richard's we understand that new technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people 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.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, 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
- 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.

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 (e.g. Behaviour Management Policy, Friendship and Anti-Bullying Policy and Child Protection and Safeguarding Policy).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. Pupils will learn about these areas in both PSHEe and ICT lessons.

2. Scope of the Policy

This policy applies to all members of the school community (including staff, governors, parents / carers, visitors) 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 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 out of school, but is linked to membership of the school.

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.

3. Policy Statements

3.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways: (depending on pupil age)

- A planned e-safety programme is provided as part of ICT / PHSEe and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutor activities
- Pupils 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
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

3.2 Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

- Website, VLE, newsletters, letters.
- Parents evenings.
- Reference to external sites.

3.3 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 formal e-safety training will be made available to staff. An

audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy.
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / pastoral care meetings / departmental meetings.
- The E-Safety Coordinator (or Safeguarding Lead) will provide advice / guidance / training as required to individuals as required.

3.4 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 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. Similar precautions and practice should also apply to homework which is directed to the internet.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit.
- Where pupils are asked to research the internet (for home especially), guidance is given to keep them on safe sites, and also so that they do not get 'lost' (spending large amounts of time looking for something).
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination, etc.) that would normally result in internet searches being blocked. In such a situation, staff can request that the E-Learning Team can temporarily remove those sites from the filtered list for the period of study. Any request to do so is auditable with clear reasons for the need, with staff requesting action through the helpdesk system.
- Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

3.5 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 e-safety technical requirements.
- There will be regular reviews and audits of the safety and security of school ICT systems by the Network Manager, which will be presented to LMT.
- 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 Network Manager and

will be reviewed, at least annually.

- All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 90 days.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Principal 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 username and password; 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.
- Users' accounts will be deleted when a user ceases employment with the school. Any data will be deleted and the associated email account will be inactive.
- The school maintains and supports a managed filtering service.
- In the event of the E-Learning Team (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 Principal (or other nominated senior leader).
- Requests from staff for sites to be removed from the filtered list will be considered by the E-Learning Team. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly
- The E-Learning Team 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.
- The Network Manager and Assistant Network Manager must ensure that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- No executable files may be downloaded by users.
- Staff are not allowed to install programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- The use of memory sticks and removable devices is not permitted by pupils; the VLE should be used for sharing and accessing teaching and learning material.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. [Accessing such information on the SLG is considered a secure connection].

3.6 Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but are responsible for any data. They must follow school policies concerning the sharing,

distribution and publication of those images. Those images must only be taken on school equipment; the personal equipment of staff must not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents / carers will be obtained before photographs of pupils are published on the school website (this is covered by the parental consent which each parent signs when their child is admitted to the school).

CCTV is used at the college for the following uses:

- As a method of controlling access
- An aid to site management in monitoring incorrect parking, manoeuvring vehicles, delivery arrivals etc.
- Student behaviour issues/bullying
- To monitor personal safety
- To monitor site safety
- As an effective deterrent for crime
- As a means of crime reduction

3.7 Responding to Incidents of misuse

Any reports should be passed on to the E-Learning Team who will consider the appropriate course of action. Breaches of this policy will be dealt with at a level appropriate to the seriousness of the alleged misconduct. Sanctions may include suspension/removal of Internet access, suspension / removal of network account and/or any normal school sanctions. Where necessary, external agencies may be involved.

- Staff procedure if pupils have inappropriate material on their mobiles
- Reporting incidents of lost information

3.8 School Filtering Policy

The school connects to the internet via the Local Authority. They filter the content before the school's systems. The school has filtering software and has responsibility for those areas which it has requested the Authority to un-blocked.

Sites can be requested to be unblocked from the Authority only by the Network Manager and Assistant Network Manager with the senior member of staff. If a member of staff wishes a site to be unblocked, they should submit the request and the reasons for this to the Network Manager. This will need to be approved by the Network Manager or Assistant Network Manager and the senior member of staff and then the request passed on if appropriate. If the site is one which the school's filtering controls, then the senior member of staff and the Network Manager must agree before any site is opened up.

3.9 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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 and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access, VLE).
- 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 pupils 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.*
- Pupils are taught about email safety issues, such as the risks attached to the use of personal details. They are be taught strategies to deal with inappropriate emails and reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	*				*			
Use of mobile phones in lessons				*				*
Use of mobiles phones in social time		*						*
Taking photos on mobile phone or other camera devices		*				*		
Use of hand held devices eg Tablet, PDAs, PSPs		*				*		
Use of personal email addresses in school, or on school network				*				*
Use of school email for personal emails				*				*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites				*				*
Use of blogs	*						*	

3.10 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 safe keeping 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 (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

4. Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

4.1 Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

4.2 Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

4.3 Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

4.4 Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

4.5 Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

4.6 Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

4.7 Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

4.8 Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

4.9 Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

4.10 Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

4.11 Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

4.12 Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

4.13 Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you

have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

4.14 Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

4.15 Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

4.16 Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

4.17 Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

4.18 The Education and Inspections Act 2006

Empowers Headteachers, 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.

5. Links to other organisations or documents

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

CEOP – (Child Exploitation and Online Protection Centre)
http://www.ceop.gov.uk/

CHILDNET
http://www.childnet-int.org/

Cyberbullying.org - http://www.cyberbullying.org/

DATA PROTECTION AND INFORMATION HANDLING
Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

East Sussex County Council – Cyberbullying - A Guide for Schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

NATIONAL EDUCATION NETWORK
E-Safety Audit Tool: http://www.nen.gov.uk/e-safety/

NORTHERN GRID
http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835

ThinkUKnow
http://www.thinkuknow.co.uk/

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

6. Resources

Further information leaflets and teaching resources, including films and video clips – for parents and school staff are available below.

Links to other resource providers:

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Chatdanger - http://www.chatdanger.com/

Digizen – cyber-bullying films: http://www.digizen.org