St. Cuthbert's
Roman Catholic High School

WHOLE SCHOOL POLICY & PROCEDURES

ONLINE SAFETY POLICY

Mission Statement

'The Lord God requires of us that we should help others whenever we can, always make the right choices and be the best that we can be in everything that we do'.

Policy: Online Safety Policy		
Type: Statutory Policy	Website: Yes	Author: Mrs C Hunt
Approved: June 2020		Next Review: June 2021
Frequency: Annual		Delegated: Full Governors or committee
Notes:		

CONTENTS

1. AIMS

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Set out clear roles and responsibilities.

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. ROLES AND RESPONSIBILITIES

3.1 The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Geraldine Cockcroft.

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputy DSLs are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy
- Updating and delivering staff training on online
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Governing Board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems daily
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects and personal development where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. CYBER-BULLYING

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes during personal development lessons and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents via social media and email, in addition to this a copy of Digital Parenting is also distributed each year.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Form time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety. .

This policy will be reviewed every year by the DSL and Network Manager.

At every review, the policy will be shared with the Governing Board

13. SOCIAL MEDIA GUIDANCE

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 photos on any social networking space. They should consider how public the information is and consider using private areas.

- 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 invite known friends and deny access to other. 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.

14. E-MAIL

- Students and staff must only use approved e-mail accounts on the school system for work related issues.
- 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.
- Use of words included in the Securus or Impero 'banned' list will be detected, logged and acted upon through the pastoral system.
- Excessive social e-mail use by students can interfere with learning and may be restricted.

Appendix 1: Student AUP

St. Cuthbert's
Roman Catholic High School

Pupil Acceptable Use Policy & e-Safety Rules

ICT and the related technologies such as the Internet and email are an important part of learning in our school. The school has a number of systems in place to protect and safeguard pupil's use of the school's ICT facilities and use of the Internet. Any attempt by a pupil to disable or circumvent these systems will result in the said pupil's access to the Internet and or school network being revoked.

We operate a very open system, allowing pupils to use programming languages and other software not usually found on school ICT systems. In return we expect pupils to not abuse this freedom that is provided. Where pupils continually abuse this trust their profile will be locked down and in persistent cases access removed from the school's network completely.

1. I will only use the school ICT systems including the Internet, email, digital video etc. for school purposes, any use of software not directly available via the start menu is strictly forbidden.
2. I will only access the school network using my own user name and password.
3. I will follow the rules of the school ICT security system and not reveal my passwords to anyone.
4. I will use only my school email address on the school system.
5. I will make sure that all ICT communication with other pupils, staff or other adults is responsible and will not cause annoyance, inconvenience or anxiety.
6. I will not send material that could be considered offensive or illegal to pupils, staff or others.
7. I will not corrupt or destroy other peoples' data, nor violate their privacy, nor will I attempt to access the computers file system or registry for activities which have not been defined by my teacher.
8. I will not disrupt the work of others nor deny them access to the network.
9. I will not deliberately introduce viruses/malware onto the network, nor will I attempt to gain access to other computers on the network.
10. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
11. I will not attempt to bypass any of the school e-safety or filtering systems, this includes but is not limited to Securus, Impero, Smoothwall or Watchguard.
12. I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
13. 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.
14. I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available to staff and or the Police if the need arises.
15. 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 will be contacted, continued breach of these rules will result in my profile being locked down and freedoms granted to all students within the school removed.
16. I understand that the statements above govern my use of on external ICT systems such as remote access as well as internal ICT systems.

PARENT/CARER AND PUPIL SIGNATURES

We have discussed this policy and I agree to follow the e-Safety Rules and to support the safe use of ICT.

Pupil name(please print) ..... Form.....

Pupil Signature .....

Parent/Carer Signature .....

Date .....

PLEASE COMPLETE AND RETURN ASAP

Appendix 2: Staff AUP

St. Cuthbert's

Staff Acceptable Use Policy / Code of conduct /Data Security/Professional Standards

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only access the computer system with the login and password I have been given and not leave ICT systems unattended when my user account is being used to access system resources.
- I will not access other network user's files unless specifically authorized to do so.
- I will ensure that all electronic communications with Students and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business, this includes using the Encrypt function when necessary.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to Students or colleague's material that could be considered offensive or illegal.
- Images of Students will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help Students to be safe and responsible in their use of ICT and related technologies.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols, including retention periods.
- I will not connect a computer or laptop to the network / Internet that does not have up-to date version of anti-virus software.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only use LA systems in accordance with any corporate policies.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

1. I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school. I have read and understood the e-Safety/Security Policy.
   I agree ☐ I do not agree ☐

2. I agree that the school can use my biometric information (such as thumbprint) to enable me to use systems such as the canteen tills and print systems, if I do not agree to this, then a smart card or pin will be provided instead. I Agree ☐ I do not agree ☐

3. I confirm that I have accessed and read and understood the latest version of the Safe Working Practice Document (that is stored on the school's website www.acrchs.net under Policies). Tick to confirm ☐

Signature .....

Date .....

Full Name ..... (Printed)

Privacy Policy: The information contained within this document will be stored against your user information in the Sims Database at may be used in evidence.