Online safety Policy

St Richard Reynolds Catholic College

Policy: Online safety
Date of publication: March 2018
Date of approval by Governing Body: March 2018
Date of next review: As required

Rationale

Our priority as a community is keeping children safe whilst allowing them the freedom to explore, to make mistakes and to learn about risks for themselves. We aim to raise awareness of safe use of the internet and related technologies. It is our responsibility to encourage safer use of online and mobile technologies by children and young people, as well as encouraging appropriate behaviour and safer practice.

We aim to embrace new and developing technologies, and actively invite innovative methods to allow our pupils to access information and engage in learning. We also aim for each member of our community, staff and pupils alike to use technology responsibly.

Aims

The aims of this policy are to:

- safeguard and protect the children and staff of St Richard Reynolds Catholic College
- enable pupils to use new technologies safely and responsibly;
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use;
- establish clear structures to deal with online abuse such as cyber-bullying;
- ensure that all members of the College community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Scope

This policy applies to all members of St Richard Reynolds Catholic College community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of College ICT systems, both in and out of St Richard Reynolds Catholic College.

This policy should be read in conjunction with our Child Protection policy, Anti-Bullying policy and Behaviour policy.

The main areas of risk for our College community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games, substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- inaccurate on-line content or lack of authenticity of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (infringement of intellectual property rights, such as music and film)

How we will achieve these aims of this policy

We will achieve these aims by:

- teaching pupils about online safety in PSHCE and other areas of the curriculum;
- ensuring that pupils know how to report online safety concerns;
- ensuring staff have up-to-date knowledge of how to help pupils to be safe;
- ensuring that staff choose suitable materials and model good on-line practice for pupils;
- working closely with parents on online safety, including an annual online safety workshop for parents;
- using of web filtering tools and usage reporting, including Impero for PC monitoring;
- having clear rules on mobile phones, social network sites and ICT facilities;
- ensuring that all pupils sign an acceptable usage agreement (see Appendix A) and this is revisited each year (e.g. in planners, in form time);
- publicising advice for online safety in classrooms and on the College website;
- ensuring that staff sign an acceptable usage agreement (See Appendix B);
- maintaining an online safety log
- monitoring online safety incidents to inform future PSHCE and training

Mobile phones

Mobile phones are allowed to be brought to College by our pupils:

- pupils are not allowed to use the phone during the College day (e.g.texting, photography, internet usage) unless a teacher has given permission;
- a teacher may, for learning purposes, allow the pupils to use their phones for a specific reason (photography, accessing internet, using apps or listening to music). The pupils will be given clear instructions to follow in these instances;
- a pupil is not allowed to contact anyone via phone call, text, social networking or email during the College day. This includes parents. Pupils may contact parents, in the case of an emergency, by using a phone in the College Office;
- parents are also not allowed to contact their child on a mobile device during the College day. Any message during the College day needs to go through the College office;

- breaches of these rules may lead to confiscation of the phone. It will be kept in a safe and will be returned in line with the Behaviour for Learning Policy;
- mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Social Network sites

Social Networking is a difficult area for any school to police as pupils usually access social networking outside of College. We therefore advise parents to monitor closely how these websites are used and how much.

Pupils must not:

- use a social network site during the College day, either on their device, or a device belonging to the College
- make defamatory comments about our pupils, staff, governors, parents/ guardians or property on a social network site, either at home or at College
- record or post any photograph or video that contains images of our staff, pupils, uniform, logo, property, or equipment without consent from the Principal.

If pupils do use social media inappropriately, sanctions will be used in accordance with the College Behaviour Policy. Where the pupil's behaviour amounts to cyber-bullying, the College Anti-Bullying Policy will be applied. The College will refer serious matters to the police.

The College encourages staff to use Twitter. However, staff should be mindful that pupils are not eligible for a Twitter account before the age of 13. Staff should also be mindful ofthe need to protect children's identities online: if photos of pupils are used, names should not be used. Staff must also be mindful of their own actions and abide by the College Acceptable Use Agreement.

ICT facilities

Pupils have access to computers, laptops, smart-boards and tablets, with a whole host of educational applications. Pupils can create written work, create art, photography, film and animation, research topics, watch educational clips, create and participate in research surveys. Pupils are not allowed to damage or misuse our property.
In particular, pupils must not:

- physically damage our equipment (e.g. throwing/ dropping/ scratching/ dismantling);
- re -programme settings to make devices hard/ impossible to use;
- change settings on any device without instruction from a member of staff;
- personalise desktop images in an inappropriate manner;
- research inappropriate subjects and materials;
- take photos of other pupils or staff and save on College ICT facilities without permission;
- search for or view inappropriate images or videos.

Sanctions for damage and misuse of our property will be given in line with the College Behaviour Policy. Staff issued with ipads must also comply with our College ipad policy.

Internet Access, Security and Filtering

The College:

- uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming and sites of an illegal nature;
- uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils;
- uses USO FX to send to send confidential material over the Internet;
- works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- is vigilant in its supervision of pupils' use, as far as is reasonable.

Network Management

The College:

- uses individual, audited log-ins for all users (on PCs) - the London USO system;
- uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- ensures the systems administrator is up-to-date with LGfL services and policies;
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems;
- has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- uses the DfE secure s2s website for all CTF files sent to other schools;
- has a wireless network secured to industry standard Enterprise security level/appropriate standards suitable for educational use.

Online communication and cyber bullying

St Richard Reynolds Catholic College treats any form of unkindness or bullying as a serious matter, and strives to promote responsible methods of communicating. We will investigate any incidents of bullying, through technological methods or otherwise, and respond in accordance with our College Anti-Bullying policy. The College takes bullying seriously and will make every effort to combat it because we believe that pupils have the right to learn in a supportive, caring and safe environment without the fear of being bullied. If cyber- bullying occurs outside College hours involving pupils, the College should be notified by contacting their child's form tutor or pastoral leader.

Parents

Our College rules on online safety have the most impact if responsible use is promoted by parents and carers at home. Parents are asked to read the acceptable use agreement with their pupils. Parents are strongly advised to monitor internet usage at home and to talk to their child about the Internet. If they have any concerns, about their child's use of technology, they should contact their child's form tutor or Pastoral Leader. The College provides an annual Online safety workshop for parents, providing advice and guidance on e- safety.

Pupils

The College has a clear, progressive online safety education programme as part of the PSHCE curriculum, which covers a range of skills and behaviours appropriate to their age and experience. Pupils are reminded of their responsibilities through the acceptable use agreement and this is enforced through tutor periods, assemblies and literature (e.g. pupil planners, posters). All pupils have their own unique username and password and are advised not to share these passwords. Pupils are taught about the safety and "netiquette" of using both e-mail in both school and at home (see Appendix C).

Staff

Staff know how to send or receive sensitive and personal data and regular updates are provided on online safety and data protection. All new staff are provided with information and guidance on the online safety policy and are required to sign an acceptable use agreement. Staff are aware of the need to use school phones for contacting pupils, parents and carers.

Monitoring

All College staff have responsibility for monitoring the online safety policy. Where pupils do not use ICT in an appropriate way, we will use a differentiated and appropriate range of sanctions, in line with our Behaviour Policy. All members of the College are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively. Where necessary, support and advice is actively sought from other agencies, such as the local authority, as needed, in dealing with online safety issues. Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible. We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
Monitoring and reporting of online safety incidents takes place and contributes to development of policies and practice in online safety within the College.

Complaints

The College will take all reasonable precautions to ensure online safety. However, owing to the international scale and nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. However we will take immediate action to address issues once identified. Parents are encouraged to report inappropriate content to social media providers and, where appropriate, to make use of the CEOP button which is on the College website.

If there is a concern about inappropriate use of the internet, parents or pupils should raise it with their form tutor in the first instance.

Any complaint about staff misuse is referred to the Principal. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with College child protection procedures.

APPENDIX A - Acceptable use agreement for pupils

ONLINE SAFETY

All pupils use computer facilities including internet access and new technologies as an essential part of learning, as required by the National Curriculum. Both pupils/students and their parents/carers are asked to sign to show that the online safety Rules have been understood and agreed.

Pupil/Student name:_____

STUDENT (High School students only to sign):
As a school user of the internet, I agree to comply with the school's student rules for internet use. I will use the computer, network, mobile phones, internet access and other new technologies in a responsible way at all times and observe all the restrictions explained to me by the school. I am aware that network and internet access may be monitored.

Student signature: _____

Date_____

PARENT/CARER:
As the parent/carer of the pupil/student named above, I grant permission for my child to use electronic mail and the internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable and that the school cannot be held responsible for the content of materials accessed through the internet. I will support the standards set by the school for my child to follow when selecting, sharing and exploring information and media electronically.

Parent /Carer Signature: _____

Date_____

Pupil/Student Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
3. I will only edit or delete my own files and not view, or change, other people's files without their permission.
4. I will keep my logins, IDs and passwords secret.
5. I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
6. I will only e-mail people I know, or those approved by my teachers.
7. The messages I send, or information I upload, will always be polite and sensible.
8. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
9. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.
12. I am aware that some websites and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk. In particular, I will not access hateful, racist or extremist material online
14. I will report any breach of online safety rules to a member of staff
15. I am aware of the e safety rules in every classroom and follow these rules when using computers.

I have read and understand these rules and agree to them.

Name: _____

Signed: _____

Form: Date: _____

Appendix B - Staff Acceptable Use Agreement

Covers use of all digital technologies in school: i.e. e-mail, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I have read and I will follow the St Richard Reynolds Catholic College online safety policy (including mobile and handheld devices).
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems, or any other / Local Authority (LA) system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with College procedures.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school approved e-mail system for any school business, including communication with parents. This is: LGfL StaffMail. I will only enter into communication regarding appropriate school business.
- I will only use the school's approved systems to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to a member of the Leadership Team.
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not connect any device (including USB flash drives) to the network that does not have up- to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's Sophos anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the teaching shared drive.
- I will follow the school's policy on use of mobile phones / devices at school and will only use them in staff areas.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- 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 access school resources remotely (such as from home) using the LGfL / school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption / USO-FX, and that I follow school data security protocols when using any such data at any location. I will not e mail unprotected pupil data externally.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the designated person (AMU) if I feel the behaviour of any child may be a cause for concern.
- I will only use any other/LA system I have access to in accordance with its policies.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Principal on their request.
- Staff that have a teaching role only: I will embed the school's online safety / digital literacy curriculum into my teaching.

User Declaration

- I agree to abide by all the points above.

- I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

- I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the school's most recent online safety policies.

- I understand that failure to comply with this agreement could lead to disciplinary action.

Signature _____

Name _____

Date _____

APPENDIX C – Classroom display poster

10 Rules for Online Safety

1. **Keep telephone number, address, name/location of school, parents' work address/telephone number private.**

2. **Report any information that makes me feel uncomfortable to my parents or my teacher.**

3. **Never agree to get together with someone you "meet" online unless my parents agree and come with me to meet them in a public place.**

4. **Never send a person your picture or anything else without first checking with my parents.**

5. **Never respond to any mean or unkind messages. Tell parents/teacher if any messages make you feel uncomfortable.**

6. **Set up rules for going online with your parents about the time of day, the length of time and appropriate areas for you to visit and stick to them!**

7. **Never give out internet passwords to anyone (even my best friends) other than parents.**

8. **Check before downloading or installing software or doing anything that could possibly hurt the computer or jeopardise your family's privacy.**

9. **Be a good online citizen and do not do anything that hurts other people or is against the law.**

10. **Help your parents understand how to have fun and learn things online. Teach them about the tech you are using!**