Online Safety Policy

St Richard Reynolds Catholic High School

Policy: Online Safety
Date of publication: November 2022
Date of approval by Governing Body: November 2022
Date of next review: October 2023

Rationale

At St Richard Reynolds we want our children to be equipped with the relevant knowledge that will prepare them for the world of tomorrow. We embrace the constant changes children face in the modern world and seek to teach them the tools they may need to grow with the fast pace of today's technological advancements.

As a Catholic school, the teachings of the gospels are at the heart of everything we do. This leads our Computing curriculum to be rooted in love for one another and teaches our children to use technology safely and respectfully, demonstrating responsibility for themselves and others through their use of information technology.

The purpose of this document is to provide a clear Online Safety Policy (relating to, but not restricted to, provision of Computing, anti-bullying and child protection) for the staff, pupils and parents of St Richard Reynolds Catholic High School, hereafter named 'the school'.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, governors and visitors) and for use both in and out of the school.

The Education and Inspections Act 2006 empowers the Head teacher to such an extent as is reasonable, to regulate the behaviour of pupils when they are on the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying (cyberbullying) or other online safety incidents covered by this policy, which may take place out of the school, but is linked to being a member of the school.

The school will deal with any incidents that fall under the remit of this, the anti-bullying and the safeguarding policies and will inform parents of incidents of inappropriate online behaviour that take place out of school.

The school's Computing Coordinator and Leadership Team (LT) will hereby act as Online Safety Coordinators.

It is to be agreed by senior management and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

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

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies 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
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- 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.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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.
    - Online safety checks are conducted 24/7 via:
        - Sophos: AntiVirus & Policy based filtering. (Sophos is managed by our on site IT team and is constantly updated by Sophos for Global Threats.)
        - LGFL: WebFiltering & Firewall protection for network traffic. (LGFL provided services are controlled by LGFL at their core data centre.)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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.

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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 and anti bullying policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher or DSL 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 (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

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 (appendix 4).

Educating pupils about online safety

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

All schools have to teach:

Relationships education and health education in High Schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of High School**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

How does internet use benefit education?

Benefits of using the Internet in education include (but are not limited):

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- a range of tools to enable, track and analyse assessment;
- a range of resources to support learning and reading;
- a range of resources to support home-school communication, such as homework activities;
- to support and enhance school-parent communication;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils using the London Grid for Learning's Net Sweeper filtering system.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti-bullying policy.)

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. This will be achieved through termly lessons which explicitly focus on cyberbullying and e-safety.

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. Class teachers will discuss cyber-bullying with their classes and integrate it within our catholic social teaching (CST) principles.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, 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/bulletins on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. An external speaker is brought in regularly to complete a workshop with parents on Online Safety.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- undermine the safe environment of the school or disrupt teaching, and/or
- commit an offence

If inappropriate material is found on the device, it is up to the DSL and/or headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The Department for Education's latest guidance on searching, screening and confiscation
- UK Council for Internet Safety's (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

ICT facilities

Pupils have access to chromebooks, 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.

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 personal data 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.

Authorised Internet Access

- The school will hereby maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign to agree to follow school IT procedures before using any school computer resource.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be entitled to annual information evenings regarding internet safety.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the IT Support Department, via their class teacher or a responsible adult.

- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school's filter system blocks sites which are inappropriate in content.

Email

- For future reference:
    - Pupils may only use approved email accounts on the school system.
    - Pupils must immediately tell a teacher if they receive inappropriate email messages.
    - Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group email addresses should be used in school by pupils
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Parents are to use the year group email to contact teachers. Staff emails should be sent from staff email addresses only and parent email addresses should not be shared or utilised by staff outside of their professional capacity.

Social Networking

- School access to social networking sites and newsgroups is blocked unless a specific use is approved.
- **Pupils will be reminded of the various age restrictions limiting their use of social media and any use of underage social media by a pupil should be communicated to parents immediately and logged with the relevant forms in school.**
- Children and parents should be made aware of the age restrictions of Social Networking sites through Online Safety lessons and editions of the High School bulletin.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Parents should not put information about school on Social Networking sites and they should not be used as forums for discussing incidents that have happened at school.

- Parents should not put photos or videos taken at school on social networking sites. This should be communicated before any event to which parents attend by staff and every effort should be made by the school to make copy-protected photographic and video material of such events available to parents at a reasonable price.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.

Video Conferencing

- Video Conferencing should only occur under the direction of a class teacher following appropriate vetting of the other party(ies) on a large screen where all children can be monitored.
- Videoconferencing will be appropriately supervised for the pupils' age.

Use of mobile devices in school

Pupils in UKS2 may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group 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 (see appendices 1 and 2).

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.

- Mobile phones will not be used by pupils for personal use during lessons or formal school time or by staff during lesson time. The sending of abusive or inappropriate text messages is forbidden by all and all content viewed via a mobile device during school time, even a personal device, should be appropriate content for a school. Staff should also be aware of how their personal device is used outside of school and the repercussions this may have if brought into school.

Published Content and the School WebSite

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will exclude those children without photographic permission through cropping when directing the shot or in post-production.
- Images may include those on the school website or to evidence work.
- Photographs should be taken on a school camera or ipad. Members of staff should not use their own mobile phone to take photos of children.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available in line with the College's Data Protection Policy.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by a member of the leadership team.
- Any complaint about staff misuse must be referred to the head-teacher. In the case that it is the head-teacher it must be referred to the governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. See Safeguarding Policy
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 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.

Communication of Policy

Pupils

- Rules for internet access will be posted in all classrooms and shared work spaces.
- Pupils will be informed that internet use will be monitored.
- If using the internet at home, pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to, both at home and in school.

- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

Staff

- All staff will be given the School Online Safety Policy and its importance explained.
- All staff must read and sign the 'Staff Code of Conduct' before using any computing resource.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should maintain a professional relationship with both parents and pupils.

Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.
- E Safety workshops to be offered annually.
- The school will ask all new pupils/parents to sign the parent/pupil agreement when they register their child with the school.
- Parents/pupils will also be asked to sign the agreement form on an annual basis.

Appendix 1 (remove this heading before printing)

E-Safety Rules

As part of the framework and programme of activities to support children's learning and development, your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. These resources include access to:

• Computers, Internet, email, digital cameras and copying and printing facilities and programmable devices

We recognise the important contribution and value that such resources play in promoting children's learning and development; however, we also recognise there are potential risks involved and therefore pupils are taught the importance of e-Safety and staying safe online.

Please see attached our basic e-Safety rules. In order to support us further in developing your child's knowledge and understanding about online safety, please read the rules with your child.

We then ask that you and your child 'sign' and return the attached Online Safety Acceptable Use Agreement. We understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful partnership.

Hopefully, you will also find the e-Safety rules provide you with an opportunity for further conversations between you and your child about safe and appropriate use of the online and digital technologies, both within and beyond the school environment, such at a friend's house or at home.

Appendix 2
Online Safety Acceptable Use Agreement

Pupil Agreement

Child's Name: ……..

- I understand the agreement for using the internet, email and online tools, safely and responsibly.
- I know the adults looking after me will help me to stay safe and check that I am using the computer to help me with my work.

Child Signature: …….

Date: ……

Parent/Carer Agreement:

- I have read and discussed the agreement with my child and confirm that he/ she has understood what the rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using online and digital technologies.
- I understand that whilst my child is using the internet and other online tools outside of the school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent Signature: …….

Date: ……

Appendix 3

Parent/Carer consent form and Online Safety Rules

All pupils use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the Online Safety Rules have been understood and agreed.

Parent / Carer name: ……

Pupil name: ……..…….

As the parent or legal guardian of the above pupil, I have read and understood the attached school Online Safety rules and grant permission for my daughter or son to have access to use the Internet, school email system, learning platform and other Computing facilities at school.

I know that my daughter or son has signed an Online Safety agreement form and that they have a copy of the school Online Safety rules. We have discussed this document and my daughter or son agrees to follow the Online Safety rules and to support the safe and responsible use of Computing at St Richard Reynolds Catholic High School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching Online Safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their Online Safety or e-behaviour that they will contact me.

I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's Online Safety.

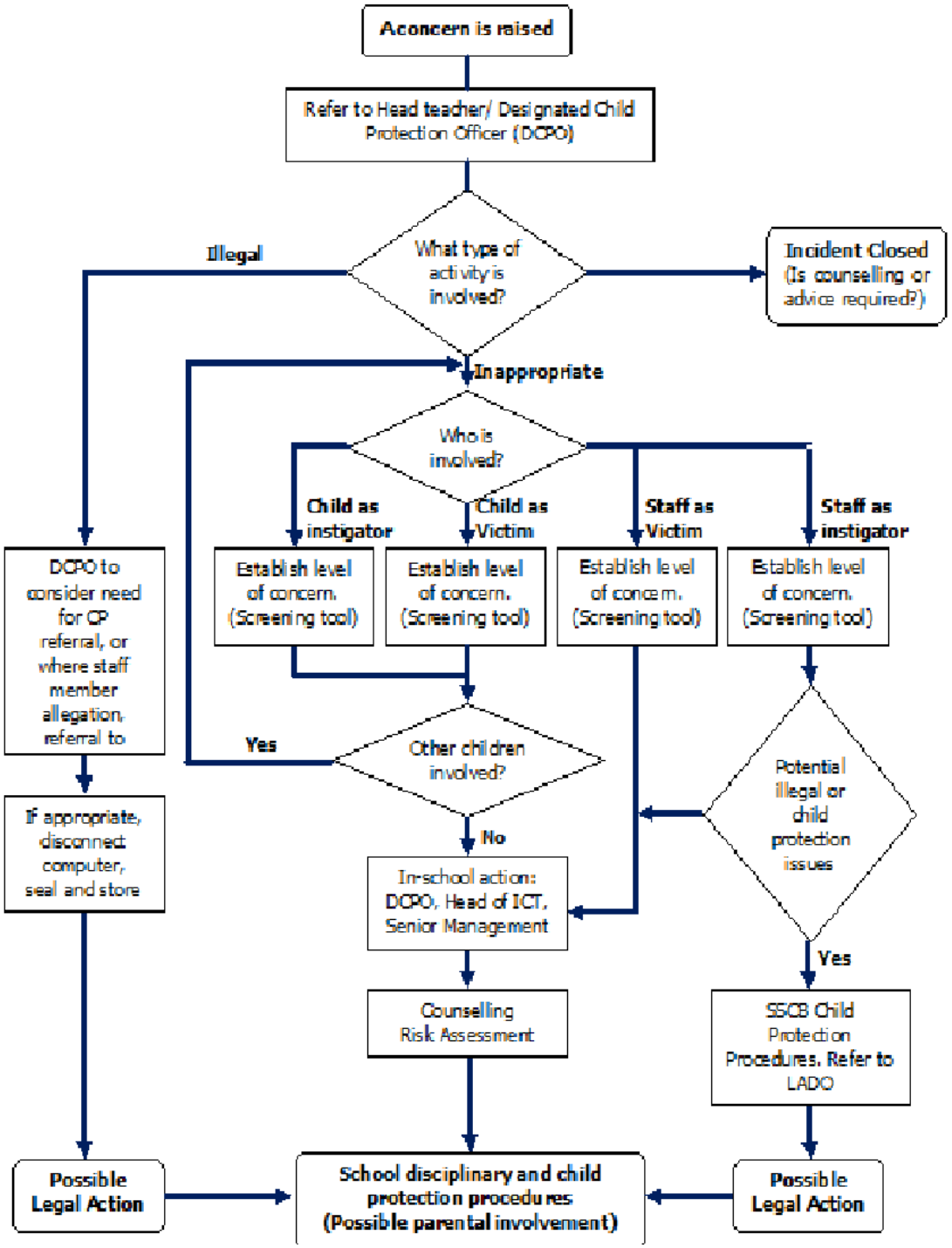
Parent/Guardian signature: ……..

Date: ……

Further information for parents on Online Safety can be found at: http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

Appendix 4

The following flow chart is to guide senior management within the School to on how to respond to an e-safety incident.



Appendix 5: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Take photographs of pupils without checking with teachers first ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**