St Edmund's Catholic Primary School

Online Safety Policy
And
Acceptable Use Agreement

Updated October 2022

St Edmund's Catholic Primary School Online Safety Policy And Acceptable Use Agreement

October 2022

ONLINE SAFETY POLICY

Introduction

- The school online safety policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.
- Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The online safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on online safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

Online Safety Policy Scope

- The school online safety policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally.
- The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding computing and Internet usage both on and off the school site. This will include imposing rewards for good behaviour and sanctions for inappropriate behaviour – as defined as regulation of student behaviour under the Education and Inspections Act 2006. 'In Loco Parentis'. Provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The online safety policy covers the use of:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School ICT equipment off-site, for example student Chromebooks, staff laptops, digital cameras and tablets
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities.
- Tablets, mobile phones, devices and laptops when used on the school site.

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety co-ordinator in our school is **Mrs Pearson**. All members of the school community have been made aware of who holds this post. It is the role of the online safety coordinators to keep abreast of current issues and guidance through organisations such Enfield LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. The online safety co-ordinator will be supported by the Inclusion Manager, as part of her responsibility for Health and Safety and Safeguarding children. The online safety coordinator/Computing Subject Leader will ensure that Governors have an understanding of the issues at our school in relation to local and national guidelines and advice; and that they remain updated.

Writing and reviewing the online safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for Computing, Behaviour, Remote Learning, Child Protection, and RHE policies including Anti-bullying.

The online safety policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year.
Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable Internet use policy or other in the light of online safety incidents.
- New guidance by government / LA / safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- Online safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police and/or Local Safeguarding Children's Board

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staff network/ staffroom
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with staff at the start of each year.

- Children to draw up online safety rules in September to be signed by all children/adults and displayed in class.

Online safety skills development for staff

- Our staff receive regular information and training on online safety issues through the coordinator at staff meetings and by the Headteacher in staff briefings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.

Online safety information for parents/carers

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website or other media.
- The school website contains useful information and links to sites like Thinkuknow, Childline, ChildNet, National Online Safety and Internet Matters.
- The school will send out relevant online safety information through letters to parents, newsletters and the school website.

Community use of the Internet

- External organisations using the school's IT facilities must adhere to the online safety policy.

Teaching and Learning
Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them.
- Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access provided by London Grid for Learning is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access
Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LGfL, Enfield LA, and any other Consultants.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' first names only will be published on the school website and will not be used in association with photographs which could be used to identify individual children.

Photographs and videos taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs/videos taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc. Parents/ carers will take full responsibility if there is any infringement of this rule.

Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept

that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are not permitted to add children as 'friends' if they use these sites.

Managing filtering

- The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, Online safety Coordinator or Headteacher.
- Leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material. Staff must follow the anti-virus protocol every time they use a memory stick in school.
- Staff are not allowed to put any information regarding pupils' details on a memory stick.
- Pupils are not allowed to bring personal mobile devices/phones to school without prior agreement from the head teacher.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff are not allowed to use personal mobile phones during designated teaching sessions.

Managing video-conferencing and remote learning

- When using Google Classroom for remote learning, please refer to the Remote Learning Policy
- When using videoconferencing via Zoom, Microsoft Teams, Skype, etc. with external agencies, it will be appropriately supervised for all pupils' age.

Protecting personal data

The school will collect personal information fairly and will let you know how the school and Enfield LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Enfield LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Enfield LA.
The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Enfield LA and as defined by the Data Protection Act 1998.
You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Policy Decisions
Authorising Internet access

- Pupil instruction in responsible and safe use will precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's online safety rules. These online safety rules will also be displayed clearly in all networked rooms.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security

- Adult users are provided with an individual network, email, Google and ScholarPack login username and password.
- Support staff should use their personal login for supply teachers and should logout of ScholarPack after they have taken the register.
- Passwords for LGfL, Scholarpack and any other application containing personal and/or sensitive information must be changed at least annually. Passwords must not be written down and stored near computers/laptops and the "Remember Password" feature of applications must not be used.
- All pupils are provided with an individual Google Classroom login username and password which also acts as a USO (Unified Sign-On) username and password to access all LGfL resources.
- Pupils are not allowed to deliberately access on-line materials, or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network and MIS systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Enfield LA can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling Online safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Strategic Leadership Team and reported to the online safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety coordinator and recorded in the online safety incident logbook.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure on the school website

Communications Policy
Introducing the online safety policy to pupils

- Online safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught in computing lessons at the beginning of every year and at relevant points throughout e.g. during RHE lessons/circle times/anti-bullying week.
- Pupils are informed that network and Internet use will be monitored**.**
- Online safety buttons will be discussed and their use encouraged when inappropriate material is displayed (for children using sites at home).

Staff and the online safety policy

- All staff will be given the School online safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Google Classroom

- All children will be given a username and password to access secure resources and facilities through Google Classroom. Children will be taught to keep this secure.
- Google Classroom will be regularly monitored for incidents of cyber-bullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that all work on Google Classroom is monitored and misuse will result firstly in a warning, followed by temporary or permanent muting should such behaviour be repeated.
- All Class Teachers will monitor the use of their own Google Classroom and ICT staff will monitor the use of ICT Google Classrooms. Any misuse will be reported to the Headteacher and an online safety pro-forma will be completed if necessary.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the online safety Coordinator.
This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the online safety Coordinator/Computing Subject Leader, Designated Child Protection Officer, and Governor with responsibility for ICT and Governor with responsibility for Child Protection. Ongoing incidents will be reported to the full governing body.
The online safety policy will be revised by the online safety Coordinator.
Date implemented: Autumn term 2021 Date for review: Autumn term 2022

Signed.....(Headteacher)

Signed.....(Online safety coordinator)

Approved by the Governing Body of St Edmund's Catholic Primary School

Signed.....(Chair of Governors)
Date:

St Edmund's Catholic Primary School

Acceptable Use Agreement

For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the children, the staff and the school.
The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- ✔ All Internet activity using school equipment and during school hours (excluding official break/lunch times) should be appropriate to staff professional activity or the children's education
- ✔ Access should only be made via the authorised account and password, which should not be made available to any other person
- ✔ Passwords for LGfL, Scholarpack, Google Classroom and any other application containing personal and/or sensitive information must be changed at least annually. Passwords must not be written down and stored near computers/laptops and the "Remember Password" feature of applications must not be used.
- ✔ Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- ✔ Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- ✔ Use for personal financial gain, gambling, political purposes or advertising is forbidden
- ✔ Copyright of materials must be respected
- ✔ Posting anonymous messages and forwarding chain letters is forbidden
- ✔ As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- ✔ Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- ✔ The use of Social Networking Sites using school equipment is forbidden in school. Social Networking sites may not be accessed using personal equipment during school hours (except in official break/lunch times). Staff are forbidden to add children from St Edmund's as "friends" to any such sites at home

Ell DigiSafe

Acceptable Use Policy (AUP) for KSI PUPILS

Name.: _____

To stay SAFE online and on my devices:

L I only USE devices oir apps, sites or games if a trusted adult says so	☐
2. I ASK for help if I'm stuck or not sure	☐
3. I TELL a trusted adult if I'm upset, worried, scared or confused	☐
4. If I get a FUNNY FEELING in my tummy, I tallk to an adult	☐
5. I look out for my FRIENDS and tel11someone if they need help	☐
6. I KNOW people online aren't always who they say they are	☐
7. Anything I do on line can be shared and might stay online FOREVER	☐
8. I don't keep Sl!i(Rffi or do DARES AND CHAUENGES just because someone tells me I have to	☐
9. I don't change CLOTHES in front of a camera	☐
10. I always check before SHARING personal information	☐
11.1 am KIND and polite to everyone	☐

My trusted adults are:

_____ at school

_____ altome

Eil DigiSafe

Acceptable Use Policy (AUP) for KS2 PUPILS

This agreement will help keep me safe and help me to be fair to others

1. *I lea.m online* - I use the,s,c:hool's internet and d,evices for schoolwonk, homework and other acti.,;1ties to learn and have,fun. School internet and deviees,are monitored.
2. *I ask permission* -Whether at home or school, I only use the devioes, ,apps, sit,es and games I am allowed to, at the times I am allowed to.
3. *I am creative onllnri* - I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make thin,gs.
4. *I am a friend online* - i won't share anything that I know another person wouldn't want shared, *or* which mi,ght upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. *I am a secure online learner* - I keep my passwords, to myself and reset them if anyone finds them out. Friends don't share passwords I
6. *I am careful what I click on* - I don't click on unexpected links or popups, and only download or install things when it has been agreed by trusted adults, Sometimes add-ons can cost money, so it is important I always check for these too.
7. *I ask Jar help if I am scared* or *worried* - I will talk to a trusted adult if anything upsets me or worries me on an app, site or game - it oftlen helps. If I get a funny feelin,g, I talk about it.

B. *I know it's not my fault if I see or someone se11dr;* me something *bad* - I won't set in trouble, but I mustn't share iL Instead, I wm tell a trusted adullt. If I m;ike a mist.ike, I don't try to hide it but ask for help,.

9. *I communicate and caflabarate online* - with people I already know and have met in real life or that a trusted adult knows about.
10. *I know new online frl'ends might not be who they say they are* - I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. *I check with an adult before I meet an online friend* face to face for the first time, and I never go alone.
12. .1 ***don't*** *do live video.s (fivestreams}* on *my own* - and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the firsttime.
13. *I keep* my ***body to*** *myseJ/ onllne* - I never set changed or .show what's under my clothes in front of a camera, I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. *I say no online 11 I need* ro - II don't have to do something just because a friend dares or challenges me,to do it, or to keep a secret. If I get asked anything that ma es, me worried, upset o,r just confused, I will say no, stop chatting and tell a trusted adult immediately.

Eil DigiSafe

Acceptable Use Policy (AUP) for KS2 PUPILS

15 ..*I fell* my *parents/r:arers what* J *do online* - they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

16. *I am private online* - I only give out private information if a trusted adult says it's okay. This might be my address, phon,e number, location *or* anything else that could tdentify me or my family and friends; if I tum on my location, I will remember to tum it off again.

17..1 *am careful what* I *share and protect my online reputation* - I know anything I do can be shar,ed and might stay online forever (even on Snapchat or if I delete it).

18. *I* ***am a*** *role-follower online* - I know that apps, sites and games have rules on how to behav,e, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.

19.*I* ***am not a*** *bully*- I do not post, mak,eor share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

20.1***am part of a*** *community*- I do not make fon of anyon,e or eKdude them because they are, different to me. If I see anyone doing this, I tell a trust,ed adult.

21. *I respect people's* ***work*** - I only edit or delete my own digital work and only use words,, pictures or videos from other people if I have thefr permission or if it is copyright free or h;,,s a Creative·Commons licence.

22. .I *am a reseQrc:her online* - I use safe search tools approved by my trusted adults. I know i can't believe everything I see online, know which sites to trust, ,rnd know how to double check information I find.

I have read and understood thi. agreement.

Signed: _____ **ID ate:** _____

lif I have any questions, I wi lll speak to a trusted adult: at school tha,t includ'es

_____

Outside school, my tru,sted adub are _____

Anti-Virus Protocol:

Perform a right-click scan on the removable device.

- **Go to Start and This PC**
- **Select the device you want to scan.**
- **Right-click and from the menu select 'Scan with Sophos End Point' and click yes.**
- **Tell David or Yvonne if there is a problem!**