Corpus Christi Catholic Primary School

Online Safety and Acceptable Use Policy

*Joyfully, unique in Jesus' family, we learn to use our special gifts to love, serve and make the world a better plac*e.

Online Safety Policy			
Approval		Board of Governors	
Chair of Governors	Anna Murphy-Sullivan	**Headteacher**	Simon Lennon
Date of last review	Nov 2024	**Date of review**	Nov 2025
Date of next review	Nov 2026	**Maintenance**	SSD Committee

Principles

It is the entitlement of every pupil to have access to the internet and digital technologies in order to enrich their learning. Use of the internet is also part of the Computing National Curriculum.

Staff and other adults working with pupils at Corpus Christi show vigilance to ensure the pupils stay safe online. They model and teach the pupils to be respectful and responsible towards others in their use of technology. They help pupils learn from mistakes or errors of judgement they may make and teach them to be safer and more responsible in the future. Embedding online safety teaching across the curriculum is considered effective practice and is vital to ensuring that pupils can navigate the online world safely and positively.

This policy should be read in conjunction with the guidance set out in Keeping Children Safe in Education (KCSiE) Sept 2025

Aims

All the pupils will:

- learn to use the internet and other digital technologies safely and responsibly
- use the internet and other digital technologies to support, extend and enhance their learning
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies
- develop a positive attitude to the internet and develop their IT/Computing capability and confidence through both independent and collaborative working
- develop an understanding of intellectual property and copyright

Pupil Acceptable User Agreement

Each pupil will complete a google form at the beginning of each academic year on google classroom. Parents will be sent a message to inform them that their child has signed a Pupil Acceptable User Agreement through google classroom which they can view by logging onto their child's google account.

Pupils' use of the internet

While using the internet in school all the pupils will:

- be taught how to effectively use the internet for research purposes
- be taught to evaluate information on the internet
- taught how to report inappropriate web content
- use the internet to enhance their learning experience
- have opportunities to engage in independent and collaborative learning using the internet and other digital technologies

Pupils' use of mobile devices

With regards to mobile devices:

- Smartphones or smart devices are not permitted on the school premises by pupils (Dorset Police Advice).
- Pupils will only be permitted to have mobile phones or other personal technology in school with the permission of the Headteacher. These pupils will be required to follow the expectations stated in the Pupil Acceptable Use Agreement, and sign a pupil friendly version (Appendix 1).
- All mobile phones must be labelled, turned off on school grounds and handed to the class teacher at the beginning of the day.

- Any mobile device that is not school property or does not have permission from the Headteacher to be on the school premises will be confiscated and will be returned to parents/carers by appointment with a member of the senior leadership team.
- Exceptional circumstances to be discussed and agreed with the Headteacher.

Pupils' use of Google - and Google Classroom

All the pupils should:

- use school email addresses for school work only
- show - our school gospel virtues by responding in a respectful manner to another child's work on google classroom where appropriate or when asked to do so as part of set homework
- never post a photograph of themselves or another pupil on any social media platform including google mail and google classroom
- tell an adult in school and/or their parents if they are concerned by what they see or read on the internet
- close the laptop lid if they see an inappropriate image or content and seek help from an adult immediately.

Staff and Governor Responsibilities and Actions

All staff, volunteers, governors and other adults working at the school must model appropriate behaviour in relation to use of the internet, and must read the Acceptable Internet Agreement, (Appendix 2), before using any information communications technology on site.

All staff should:

- be trained and aware of the inappropriate use of smart devices/phones where images taken could be harmful to other children and staff (e.g. upskirting, taking and/or sharing images of peers without agreement
- contribute to the development of Online Safety policies and practices
- take responsibility for the security of confidential data
- actively teach the pupils about Online Safety during each unit of learning that involves online use
- ensure that all pupils are aware, in an age appropriate manner, that certain online behaviours can increase the likelihood of, or causes, harm (conduct)
- being aware that by being online pupils may be subjected to harmful online interaction with other users (contact)
- be aware that pupils can be exposed to material that is illegal, harmful or inappropriate (content)
- explain to children what internet use is acceptable and ensure that pupils access material that is appropriate to their age and maturity
- set clear learning objectives and expectations for internet use during lessons and ensure that internet use is embedded to support and enhance the whole curriculum
- demonstrate safe access to the web and ensure that all pupil access is supervised
- deal with Online Safety issues as they arise and be alert to potential issues / risks

Online Account Closure

- When a pupil leaves the school their account will be frozen on the day of their leaving the school. Parent/carers accounts will also be closed on this date.
- When teaching staff leave employment their email account and access to the school drive will be closed on the date of their last working day in school term time (i.e. not necessarily last day of salary).
- On the date of the last working day in school term time, teaching staff will hand in their door fob and will have returned any IT devices that they have borrowed for the purpose of school work
- Via email, the SBM (School Business Manager) and/or Premises and Infrastructure Manager will confirm with the staff member leaving which date the fob and/or IT devices will need to be

returned and when the account will be frozen.

- When non Teaching Staff leave employment: the same protocol above applies but on the last day of working on site.
- When Governors leave: they will also be subject to the online account closure procedure.

Computing/Online Safety Leader Responsibilities

- Provide guidance and resources to support other staff's use of the internet and digital technologies / devices
- Ensure frequent visits are made by the Safer Schools and Community Officers Team at Dorset Police to deliver high quality and age appropriate sessions to each year group with subsequent training being delivered to staff and to governors and parents by invitation.
- Provide frequent updates on the newsletter to parents on the latest online concerns and tips.
- Investigate and act upon any incidents reported.

Headteacher responsibilities

- Assumes overall responsibility for Online Safety issues within the school but may delegate the day to day responsibility to the Online Safety Leader.
- Ensure that developments at Local Authority level are communicated to the Online Safety Leader (including PREVENT agenda).
- Ensure that the Governing Body is informed of online safety issues and policies.
- Make all staff aware that internet traffic can be monitored and traced to the individual user and that safe, professional conduct is essential.
- Assume editorial responsibility for all content on the school website and on the school Instagram account by ensuring that it is accurate, appropriate and accessible.
- Report any material believed to be illegal to appropriate agencies such as the Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).
- Review the security of the school information systems and users regularly.

Governors

- Appoint an Online Safety link governor who will ensure that it is included as part of the regular review of child protection and safeguarding and health and safety policies.
- Support the Head Teacher and/or designated Online Safety Leader in establishing and implementing policies, systems and procedures for ensuring a safe IT/Computing learning environment.
- Ensure that appropriate funding is authorised for online safety solutions, training and other activities.

Email

- Pupils will only use approved school email addresses in school.
- Pupils will inform a member of staff if they receive inappropriate or abusive emails.
- Access to personal email accounts may be blocked if the Headteacher feels there is any infringement of the Acceptable Use Agreement for both children and adults.
- Email sent to external organisations must be written carefully and professionally.

Publishing web content

- The contact details on the school website should be the school address, admin office email address and telephone number.
- The website should respect and reflect property rights and copyright.
- Images of pupils should be selected carefully and be published only with the consent of the parents/carers and be presented in a way that reduces the opportunities for it to be reused elsewhere.
- Pupils' work can be published on school website unless parents have specifically asked for it not to be.

Managing social media

In line with KCSiE 2025 additional content area of risk for online safety are as follows:

- Misinformation
- Disinformation (including fake news)
- Conspiracy theories

Children using social media will be advised:

- to discuss their account on an ongoing basis with a trusted adult in their family
- never to give out personal details which may identify them and / or their location. Examples would include real name, address, phone numbers, school, IM (instant messages) and email addresses, full names of friends/family, specific interests and clubs
- not to publish specific and detailed private thoughts, especially those that may be considered threatening, harmful or defamatory
- not to publish photos of themselves or others online
- not to arrange to meet people who they have met online and immediately inform a responsible adult

School social media:

- The school's Instagram account managed by the Online Safety Champion and Assistant Headteacher who has responsibility for communication and marketing.The purpose of the instagram account is to promote the school through sharing news and updates with parents/carers
- All personal information, including names and photos of pupils will only be published with parental consent.
- Any staff blogs run from the school website must be agreed with the Headteacher. The school website should also centrally host any online communications between staff and pupils i.e. to support home learning tasks via Google Classroom.

Staff use of social media:

- Staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children.
- Staff should make appropriate use of the security settings available and should consult the Computing Leader for support with this if necessary.
- Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.
- Under no circumstances should any school staff have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites.
- School staff are strongly advised not to accept friendships via their social networking with parents, ex-parents and governors. Where staff do accept such friendships, they must not engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts.
- School staff are fully entitled to accept friendships with colleagues via their social networking site but should take care in communications exchanged in areas of public access.
- Senior staff and those who have line management responsibility are advised to consider the appropriateness of accepting colleagues, as contacts on social networking sites.

Parental Use of School's Social Media:

- Parent Teacher Association social media accounts must be managed in line with the

expectations set out for the school instagram account.

- Parents who use the school's systems should confirm with Appendix 3.

Internet filtering

- All stakeholders are people filtered in groups: Staff, SLT, Pupils and Governors). RM filtering is the first level filtering system and the next level is SWG. Only the Administrator will have access to the password that can bypass the filtering systems.Unfiltered sites will not be used.
- If staff or pupils discover unsuitable sites, the URL must be reported by the teacher to the Premises and Infrastructure Manager immediately and access blocked.
- Where staff bypass the filtering system, the content they wish to access must first have been screened without the children present and deemed appropriate by them using their professional judgement.

Managing emerging technologies

New IT applications, both hardware and software, will initially be explored by the Computing Leader and the School's Premises and Infrastructure Manager. Advice will then be put to the Senior Leadership Team, enabling them to assess the educational benefits and potential risks.

DfE's generative AI: product safety expectations - it is important that staff are aware of:

- How to use generative AI safely
- How filtering and monitoring requirements apply to the use of generative AI in education

Training

The school will ensure that all teaching staff (teachers and teaching assistants) have a basic understanding of Online Safety. Formal training will be provided for key staff by the Online Safety Leader or by a recommended outside agency Ongoing dialogue will support an open culture where potential issues are identified, discussed and solutions agreed.Governor responsibility to keep updated with KCSiE including online safety.

Working with parents and carers

Ensuring that children are able to use the internet safely requires a partnership approach between the school and parents/carers.

Consequently, the school will:

- ensure that this policy and the Acceptable Use Agreements are displayed on the school website
- offer annual Online Safety information for parents delivered by the school's Online Safety Leader and the SSCT
- ask parents to sign a Home School Agreement which incorporates a commitment to safe internet usage
- teach children that safe access to the internet is as important at home as it is at school
- frequently offer online safety advice via the school newsletter

Online Safety Complaints

- Staff must log incidents reported to them on MyConcern and if necessary refer the matter to the - DSL or member of the safeguarding team

- Instances of staff internet or other IT misuse should be reported to and will be dealt with by the Headteacher

Related policies

This policy should be read in conjunction with the school's Behaviour Policy, Anti-Bullying Policy, Child Protection and Safeguarding Policy and Confidentiality Policy. Any complaints relating to Online safety will be managed according to the school's Complaints Policy.

	Corpus Christi Catholic Primary School **Pupil Acceptable Use Agreement**

Corpus Christi school will try to ensure that pupils will have good access to technology to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement *(completed as a google form at the beginning of each academic year)*

I understand that I must use school computing systems in a responsible way, to ensure that there is no risk to my safety or to others.

For my own personal safety:

- I understand that the school will monitor my use of IT.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- I will tell an adult if I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable online.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language.
- I will not take or send images of anyone without their permission.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use the school IT and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g communicating with other members of the school, accessing school email, blogging, website etc.

Name of Pupil (print please) Signed Date

	**Corpus Christi Catholic Primary School** **IT Acceptable Use Agreement**

IT in its many forms – internet, email, mobile devices etc. – is now part of our daily lives. It is our duty to ensure that it is used safely and responsibly.

All Staff, Governors & Volunteers at Corpus Christi Catholic Primary School are aware of the following responsibilities:

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Passwords should be a minimum of 8 eight symbols and contain a range of characters such as upper and lower case letters, numbers, and symbols.
- That they are responsible for any activity carried out under their username.
- Hardware or software will not be installed on any school owned device without the Headteacher permission.
- Understand that the use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures.
- Report any E-safety concern to a Designated Safeguarding Leadas soon as possible.
- Never use Personal mobile phones or digital cameras for taking any photographs related to school business.
- Emails should be written carefully and politely. As messages may be forwarded, emails are best regarded as public property.
- Copyright and intellectual property rights must be respected.
- The security of IT systems must not be compromised, whether owned by the school or by other organisations or individuals.

	Corpus Christi Catholic Primary School **Conditions of use for Social Networking Sites**

Purpose

As we embrace forms of communications technology new to the school we will closely and regularly monitor their use through our e-safety champion and senior leadership team. As always, any feedback you have about such sites and their use can be made through contacting the school directly (rather than through the social networking sites themselves).

Corpus Christi Catholic Primary School will use these sites for:

- Regular news items – which will be repeated in newsletters and on the school website
- Important news which cannot wait until the next school newsletter, such as school closure or last minute change of times for assemblies
- Interesting curriculum, sports and trip news from around the school submitted by administration staff, senior leaders, teachers and children (supervised by an adult)

Misuse

We intend the communication to be one-way only, so we will not engage in conversations with parents, or other users on social networking sites. Therefore, negative or derogatory comments about the school, staff, individuals or other parents/carers and children will lead to an automatic blocking of that person to the school's pages. Persistent use of the site for this purpose by a group deemed large enough will lead to the sites being closed. We will of course be willing to listen to any feedback about the school through appropriate means.

We ask that parents and children using the site will only use it to read comments provided by the school. We do not feel the need to use many of the fun features on these sites other than the posting of messages and pictures.

Awareness

Please note that any user posting inappropriate comments is responsible for what is posted on the site under their username – ***please ensure that if you do log into social media sites that you do not leave it unattended for others to abuse your account.*** *The user of that account will be blocked even if someone else abuses their account. This includes use by children, who should only look at the site under adult supervision.*

All staff must remember that they are professionals with a duty beyond the school day so therefore when posting on personal social media sites must be mindful of the content and the possibility of other members of the school community viewing this. Should this content be deemed inappropriate there will be a conversation with a member of the Senior Leadership Team.