HOLY CROSS CATHOLIC PRIMARY SCHOOL
Company No: 07696905
Registered Office: Queen's Drive, Swindon, Wiltshire, SN3 1AR
Tel: 01793 527679
www.holycross.swindon.sch.uk
✉: admin@holycross.swindon.sch.uk

Learn, Grow, Love, Live

Online Safety Policy 2023-2026

Version	Date	Description of changes and person/organisation responsible
1.0	February 2023	Reviewed
	September 2023	Reviewed

People Responsible:	Headteacher Governing Body
Reviewed date:	February 2023
Next review date:	September 2026

Mission Statement

At Holy Cross Catholic Primary School,
we learn about ourselves and about the world.
We grow in faith,
we act with kindness, generosity and love
to ourselves and others.
We live life to the full and have a future full of hope.

1. Aims

Our school aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones');
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

What are the school's responsibilities around online safety?

This school recognises:-

- the increasing role technology has to play in education and children's daily lives
- the wide-range of content which is available to children via the internet
- that alongside the benefits of technology, there are also risks
- the importance of delivering a broad and relevant online safety curriculum which provides progression across year groups
- that delivery of this curriculum must be provided via regular lessons, which take place throughout each term
- the importance of keeping up to date with the tools, apps and devices children are using so that the curriculum which is offered is meaningful
- that online safety must be reflected in all relevant school policies
- its responsibility to work in line with the Filtering and Monitoring standards.

What our online safety curriculum offers

- Our online safety curriculum covers four aspects of risk – content, contact, conduct and commerce *(see page 35-36 KCSIE for definitions)*
- Key online safety messages (such as Childnet's SMART rules) which are reinforced at every opportunity across the curriculum, in assemblies, PSHE lessons
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and understand that not everything they see online is true
- Pupils are supported in building resilience to radicalisation. A safe environment is provided for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

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

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

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

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

3. Roles and responsibilities

3.1 The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Ensure the school has appropriate filtering and monitoring systems in place;

- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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

3.2 The Headteacher

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

The headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.

The headteacher and members of the senior leadership team (SLT) are responsible for ensuring that the computing lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. They understand the systems in place and an annual review of online safety takes place, including review of filtering and monitoring systems.

This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The SLT will receive regular monitoring reports from the computing lead.

The headteacher and members of the SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

3.3 E-Safety Coordinator (GHS Ltd)

Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

Provides training and advice for staff.

3.4 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;
- understanding and monitoring the schools filters and systems which are in place;
- 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 (Appendix 5) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- updating and delivering staff training on online 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.

3.5 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 on a regular basis;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- ensuring that any online safety incidents are logged via class log books and CPOMS and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.6 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 on CPOMS and in classroom e-safety log books 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;
- 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.'
- are aware of filtering and monitoring provisions in place and know how to respond when concerns are identified. They are provided with online safety training, at induction and at regular intervals

This list is not intended to be exhaustive.

3.7 Parents

Parents and carers play an essential role in the education of their children and in the monitoring of the children's on-line behaviours. Parents are expected to:

- notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- read the Acceptable Use Policy (AUP) and encourage their children to adhere to the guidelines;
- ensure their child has read, understood and agreed to the terms on AUP for use of the school's ICT systems and internet (Appendices 1 and 2);
- support the school in their e-safety approaches by discussing e-safety issues with their children and reinforce appropriate, safe online behaviours at home;
- model safe and appropriate use of technology and social media;
- abide by the school's AUP and identify changes in behaviour that could indicate that their child is at risk of harm online;
- seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online;
- ese school systems, such as learning platforms, and other network resources, safely and appropriately;
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

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

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

The school will seek to provide information and awareness to parents and carers through:

- letters, newsletters and the school website;
- online safety parent information events and online workshops;
- reference to the relevant web sites and publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

3.8 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 the AUP (Appendix 3).

3.9 Filtering and monitoring

See also:-
Pages 37-38 KCSIE for further information

As part of the work we do to provide pupils/students with a safe environment in which to learn, we ensure that we have appropriate filtering and monitoring systems in place. Harmful and inappropriate content is blocked without unreasonably impacting on teaching and learning.

We work collaboratively to keep pupils/students safe in the online world.

- Governing bodies have responsibility for ensuring the school has appropriate filtering and monitoring systems in place, taking into account the age of our pupils/students and those who are potentially at greater risk of harm. We have a named governor for filtering and monitoring in our school.

- Senior leaders, including the DSL have an awareness and understanding of the systems in place. An annual review of online safety takes place, including review of filtering and monitoring systems.

- Staff have an awareness of provisions in place and know how to respond when concerns are identified. Staff are provided with online safety training, at induction and at regular intervals.

- Within the four key areas of risk (Content, Contact, Conduct and Commerce), pupils/students are taught about the steps they should take if they identify illegal, inappropriate or harmful content online.

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 primary schools.

The children are taught e-safety via:

- the e-safety curriculum is planned as part of Computing and PSRHE;
- key e-safety messages are reinforced through our school website, assemblies and classroom activities. Children are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- children are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- staff act as good role models in their use of digital technologies the internet and mobile devices Internet use in lessons is pre-planned, following best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

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 primary 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.

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

At Holy Cross Catholic Primary School, we are aware that parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" (Byron Report).

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

Online safety will also be covered during parents' evenings.

The school will let parents know:

- what systems the school uses to filter and monitor online use;
- what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power (See also the school behaviour policy).

6.2 Preventing and addressing cyber-bullying

The way in which pupils relate to one another online can have a significant impact on the culture at school. Negative interactions online can damage the school's culture and can lead to school feeling like an unsafe place. Behaviour issues online can be very difficult to manage given issues of anonymity, and online incidents occur both on and off the school premises.

Even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity.

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

The school will actively discuss cyber-bullying with pupils via the Purple Mash Computing program, visitors and PSRHE curriculum. The reasons why it occurs, the forms it may take and what the consequences are discussed with the children. Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSRHE education, and other subjects where appropriate.

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

The school also sends information/leaflets 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.

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.

6.3 Examining electronic devices

Staff

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present and during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room). If walking to one of these places, their mobile phone should not be in use – this includes hours when breakfast or after school clubs are in operation.

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time. For instance:

- for emergency contact by their child, or their child's school;
- in the case of acutely ill dependents or family members;
- mobile phones are also used by teachers to enable access to CPOMS.

Phones brought into school are entirely at the staff member's, pupil's & parents/carers' or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any mobile phone or personal device brought into school.

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as child protection, data protection and AUPs.

Pupils

Children who bring a mobile phone to school must sign an agreement alongside parents that they understand the rules of use of mobile/camera technology in school. If these rules are breached, this may result in loss of privilege. Failure to adhere to this guidance will result in disciplinary action being taken

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Use of digital and video images - photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause

harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. If those images are taken on personal equipment, then they should be removed as soon as possible.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Parents or carers are offered the chance to opt out of allowing photographs of pupils to be published on the school website.

Pupil's work can only be published with the permission of the pupil and parents or carers.

9. Pupils using mobile devices in school

We recognise that mobile phones and other internet-enabled devices are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, mobile devices are capable of more than simply helping a child get in touch with parents at the end of the day. Therefore, it is incumbent upon parents to understand the capabilities of the phone/device and the potential use and mis-use of those capabilities. Holy Cross Primary School discourages children from bringing mobile phones to school if at all possible and other internet -enabled devices are not permitted, due to the potential negative issues that may arise, for example:

- mobile devices may be lost, stolen or damaged;
- mobile devices can prove a distraction to teaching and learning in school;
- they may provide a means of bullying or intimidating others;
- there are risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

If it is necessary for a child to bring a mobile phone to school, parents need to submit a request form to the head teacher. Other mobile internet- enabled devices such as an Apple watch are not allowed in school.

Children who bring a mobile phone to school must sign an agreement alongside parents that they understand the rules of use of mobile/camera technology in school. If these rules are breached, this may result in loss of privilege. Failure to adhere to this guidance will result in disciplinary action being taken.

10. Pupils using technology during partial school closure/lockdowns.

This school recognises:-

- the increasing role technology has to play in education and children's daily lives, and the increased use during times of lockdown due to Covid
- the wide-range of content which is available to children via the internet
- that alongside the benefits of technology, there are also risks

For those who are not physically attending school during partial school closure, we recognise that these pupils will be spending increased time online, either participating in school work, taking part in live streaming of lessons and/or as part of extended 'free-time' due to lockdown procedures in place nationally.

We recognise that this will pose increased risk to children, including:-

- Grooming
- Exploitation, both criminal and sexual
- Radicalisation
- Child on child abuse, including cyber-bullying
- Sexual harassment

All staff who interact with pupils/students, including remote interactions, will continue to be vigilant and look out for signs that a child's safety and welfare might be at risk. Further guidance to keep pupils/students and staff safe when working remotely can be found in Safer Working Practice (Updated February 2022)

In addition, pupils are sign-posted to age appropriate practical support should they have worries or concerns whilst online. Links to support are available via our school website and include:-

UK Safer Internet Centre Hotline

Child Exploitation and Online Protection Centre

11. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- ensuring any external hard drives or memory sticks are encrypted – this means if the device is lost or stolen, no one can access the files stored on the external hard drive or memory stick;
- making sure the device locks if left inactive for a period of time;
- not sharing the device among family or friends;
- allowing all installations of anti-virus and anti-spyware software by GHS Ltd;

- allowing all operating systems to be up to date by always installing the latest updates issued by GHS Ltd.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice GHS Ltd.

12. How the school will respond to issues of misuse

All pupils, members of staff and other adults have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that all users are fully aware of their responsibilities when using technology, they are required to read and sign the appropriate acceptable use policy.

In the event of an e-safety incident involving illegal activity, the school will:

- inform a member of the safeguarding team for incidents involving pupils, and inform the Headteacher for incidents involving staff;
- secure and preserve all evidence and hardware;
- the head teacher will report the incident to the appropriate agencies, such as IWF, the Police or CEOP;
- take internal action through the school's behaviour, anti-bullying and child protection policies, as appropriate. E-safety incidents that involve inappropriate rather than illegal activity will be dealt with through the school's behaviour, anti-bullying and child protection policies, as appropriate. A log of all reported E-safety incidents related to children will be maintained on CPOMs.

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

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

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

13. 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 DDSLs 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.

14. Monitoring arrangements

All staff can log behaviour and safeguarding issues related to online safety via CPPMs.

This policy will be reviewed every year by the computing lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Official Use of Social Media

The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes:

a) The official use of social media as a communication tool has been approved by the Headteacher.
b) Leadership staff have access to account information and login details for the social media accounts, in case of emergency, such as staff absence.

Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff use school provided email addresses to register for and manage any official school social media channels.

Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.

Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague. Official social media use will be conducted in line with existing policies, including: anti-bullying, child protection and data protection.

All communication on official social media platforms will be clear, transparent and open to scrutiny. The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

16. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Mobile Phone Policy
- Complaints Procedure

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

HOLY CROSS CATHOLIC PRIMARY SCHOOL
www.holycross.swindon.sch.uk
✉: **admin@holycross.swindon.sch.uk**

Acceptable Use Policy KS1 and Foundation Stage

I want to feel safe all of the time.

I agree that I will:

- only open pages which my teacher says are safe
- only talk to people online that I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show a trusted adult if I get a nasty message
- not reply to any nasty messages or anything which makes me feel uncomfortable
- talk to my trusted adult before using anything on a computer or tablet to make sure I am kept safe
- not play games on the computer or tablet (unless told to by my teacher) during lesson time
- not tell anyone about myself online (including my name, my family and home, phone numbers or pets)
- not load photos of myself onto the computer
- never agree to meet a stranger
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

I know that anything I do on the computer or tablet in school will be seen by a trusted adult.

I have discussed these rules with my child and they understand what is expected from them and know what to do when there is an issue.

Child's Name …… Class ……

Parental Signature…… Date……

Appendix 2: KS2, acceptable use agreement (pupils and parents/carers)

HOLY CROSS CATHOLIC PRIMARY SCHOOL
www.holycross.swindon.sch.uk
✉: admin@holycross.swindon.sch.uk

KS2 Pupil Acceptable Use Agreement

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

Safe:

I will keep my logins and passwords secret.

I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends to anyone, unless a trusted adult has given permission.

I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

Trust:

I know that not everything or everyone online is honest or truthful and I will check content on other sources like other websites, books or with a trusted adult.

I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

Responsible:

I will only edit or delete my own files and not look at, or change, other people's files without their permission.

I will only post pictures or videos on the internet if they are appropriate and if I have permission.

I will only change the settings on the computer or tablet if a teacher/technician has allowed it.

The messages I send, or information I upload, will always be polite and sensible.

I will only e-mail people I know if a responsible adult has approved this.

Understand:

I will only use the school's computers or tablets for schoolwork and homework.

I will not bring files into school without permission or upload inappropriate material to my workspace.

I am aware that some websites and social networks have age restrictions and I should respect this.

I will not attempt to visit Internet sites that I know to be banned by the school.

I understand that the school's devices are monitored.

Tell:

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 show a teacher / responsible adult.

If I am aware of anyone being unsafe with technology then I will report it to a teacher.

I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.

If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.

I know that I can visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to learn more about keeping safe online.

Name ..... Class .....

Signature ..... Date.....

Appendix 3: Acceptable use agreement (staff)

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of ICT in their everyday work. The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

Staff will be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- 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, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust GDPR Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

  • I understand that I am responsible for my actions in and out of school.

  • I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date