HOLY CROSS
CATHOLIC PRIMARY SCHOOL

Online Safety Policy

April 2021

This policy should be read in conjunction with Acceptable use of the internet policies, Child-Protection and Safeguarding, CAST Data Protection, CAST Social Media and Anti-Bullying Policies.

Roles and Responsibilities
The following section outlines the online safety roles and responsibilities of individuals and groups within our school.

Governors
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Full Governing Body who receive regular information about online safety incidents. The Curriculum and Safeguarding governors take responsibility for monitoring the policy and practices.

The Senior Leadership Team
The Senior Leadership Team has a duty of care for ensuring the safety (including online safety)of members of the school community. The day to day responsibility for online safety is taken by the online safety/computing lead, Susan Buscombe.

The Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Head teacher and Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring role

Online Safety Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority / Plymouth CAST, as appropriate
- Liaises with school technical staff

Technical staff

Technical Staff / Computing Lead is responsible for ensuring:

- That our school technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any MAT / DFE and Ofsted Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That monitoring software / systems are implemented and updated as necessary.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read and understood the Staff Acceptable Use Policy /Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher/ Deputy Head Teacher for investigation/action/sanction
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems- Class Dojo, email, text message
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies and devices in lessons and other school activities and implement current policies with regard to these devices.

Designated Safeguarding Lead

The Designated Safeguarding Lead and Deputy DSL should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- peer on peer abuse
- potential or actual incidents of grooming
- online-bullying

Teaching and Learning

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the online safety provision at Holy Cross. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing /PHSE and should be regularly revisited. The first computing lessons in each term will focus on digital literacy.
- Our digital literacy programme is based on the eight aspects of 'Education in a Connected World' and rooted in the knowledge and skills outlined in our digital literacy progression document.
- Key online safety messages should be reinforced as part of a programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials /content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, theinternet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processesare in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the online safety lead or technical staff (TME) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals, as required

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any committee involved in technology / online safety / health and safety /safeguarding. This may be offered in anumber of ways:

- Attendance at training provided by the Local Authority / Plymouth CAST
- Participation in school / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that our infrastructure / network is as safeand secure as is reasonably possible and that policies and procedures approved within this policy are implemented. All procedures are managed in line with the expectations outlined in annex C of KCSIE 2020.

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systemsand devices.
- Users are responsible for the security of their username and password andwill be required to change their password regularly.
- The Computing Lead/Administration Team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users**.** Illegal content (child sexual abuse images) is filtered by SWGfL by actively employingthe Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes
- Internet filtering / monitoring takes every reasonable precaution to ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individualworkstations are protected by up to date virus software.
- An agreed policy is in for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. They are provided with group network access.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press

  In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy events for their own personal use (as such use in not covered by the Data Protection Act/GDPR regulations). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital /video images.
- Staff and volunteers 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. Those images should only betaken on school equipment; the personal equipment of staff should not beused for such purposes.
- 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, particularly in association with photographs.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff are able to use the school email service to communicate electronically with others when in school
- Children and staff may also use the messaging and communication features within Google Classroom as a safe and secure means of communication. Children are taught to use the class stream in a polite and respectful manner.
- Staff and children need to be aware that online communications may be monitored
- Staff and children must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email, message or communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Children should only bring mobile phones into school in accordance with school policy. The phone will be handed to a member of school staff to be kept securely during the school day.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the Holy Cross or Plymouth CAST liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school/academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:
- No reference should be made in social media to students/pupils, parents/carers or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school/academy social media accounts are established there should be:
- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school/academy disciplinary procedures*

Personal Use:
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school/academy or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media:
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's/academy's* use of social media for professional purposes will be checked regularly by the senior leadership team to ensure compliance with the school policies.

Sexting

Holy Cross School ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating child produced sexual imagery (known as "sexting"). We view "sexting"as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead

The school will follow the guidance as set out in the non-statutory UKCCIS advice'Sexting in schools and colleges: responding to incidents and safeguarding youngpeople'
If the school are made aware of incident involving child produced sexual imagery theschool will:

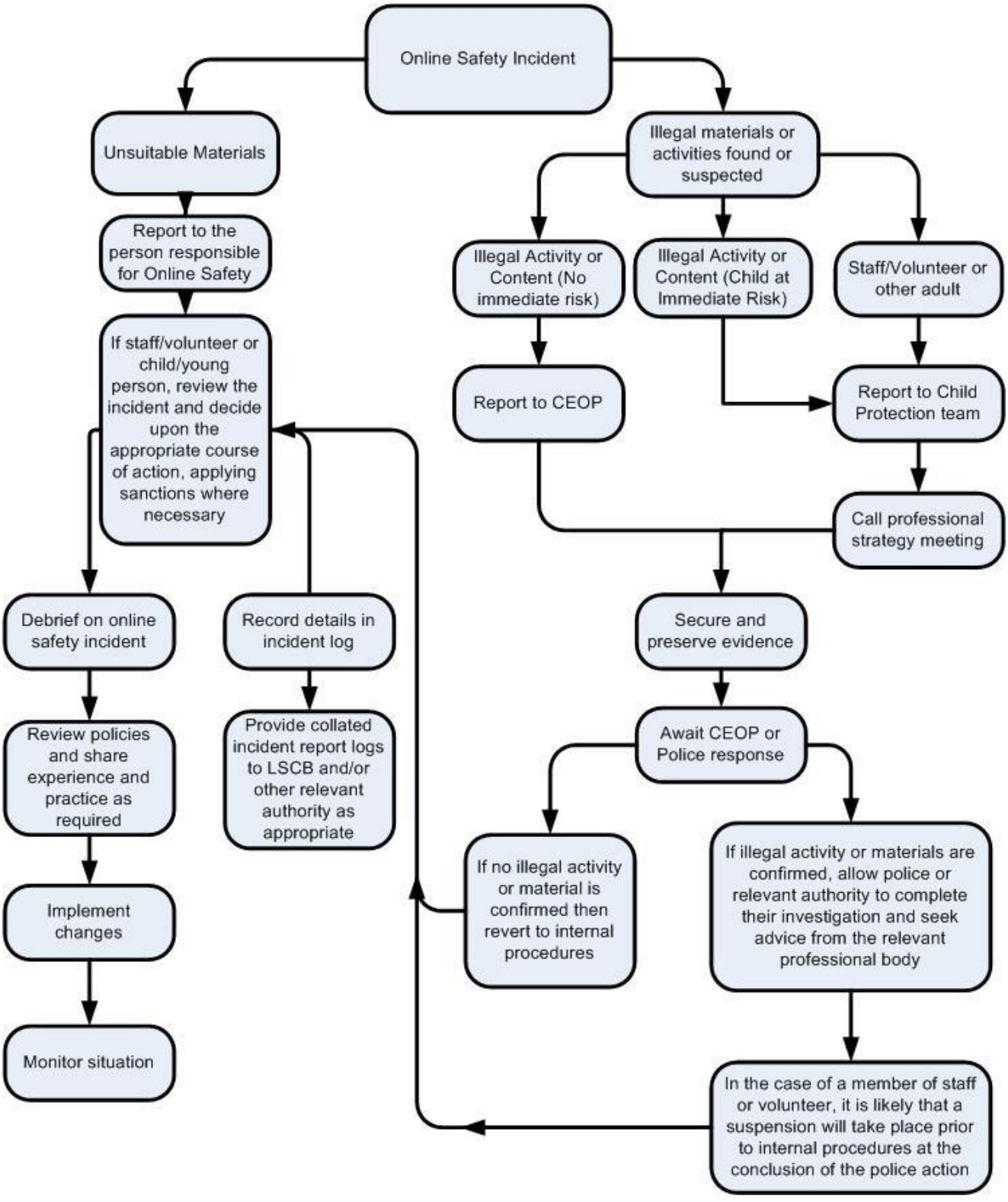
- Act in accordance with the schools Child protection and Safeguarding policy
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevantchecks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the school behaviour policybut taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.
- The school will not view any images suspected of being child produced sexual imagery unless there is no other possible option or there is a clear need or reason todo so.
- The school will not send, share or save content suspected to be an indecent imageof children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network ordevices, then the school will take action to block access to all users and isolate theimage.
- We will take action regarding creating child produced sexual imagery, regardless ofthe use of school/setting equipment or personal equipment, both on and off the premises.
- We will ensure that all members of the community are aware of sources of support regarding child produced sexual imagery

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However,there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This isvital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by children and if necessary can be taken off site by the police should theneed arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and contentvisited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record andstore screenshots of the content on the machine being used for investigation. In the case of a child record the incident on CPOMS. In the case of a member of staff record and save/print any screenshots.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriateaction will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
- Police involvement and/or action
-

If content being reviewed includes images of child abuse, then the monitoringshould be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state mayhinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The records should be retained by the group for evidence and reference purposes.

Review and Monitoring

As a school we use the 360° Safe to review our online safety policies and practices.The review framework is updated at least termly and action plans are generated to inform our practice. This framework can be accessed through www.360safe.org.uk/. The policy is monitored on a day-to-day basis by the SLT, who report to the Governing Body about its effectiveness, on request.

Policy prepared by Susan Buscombe (Deputy Head Teacher)

Approved by Governors on

Review date: April 2022

Appendix 1

Acceptable use of Live Streamed Lessons/Meetings Agreement

Live-streamed lessons form an important part of a blended approach to remote learning, providing opportunities for the enhancement of teaching and learning when pupils are not in school.

As with all online activity it is important that all participants observe correct protocols when leading or taking part in live-streamed lessons.

- 1:1 video calls with pupils will not take place.
- Video calls and meetings will only take place during normal school hours.
- Daily *screen-time* will be reasonable and proportionate for pupils and staff
- Live-streaming of lessons will be used as part of a blended approach to remote learning in which non-screen-time-work has equal value.
- The member of staff will record the length, time, date and attendance for the lesson, and a note of anything of concern that happens in the lesson.
- Parents must be aware that the video call is happening.
- Parents must provide written consent to allow their child to take part in a live streamed lesson. By signing this document the parent is providing consent for his/her child to participate in live-streamed lessons that the parent is aware of.
- Parents have the right to withdraw their consent for their child to take part in remote lessons at any time. This will be done in writing/by email to holy.cross.rc.primary.school@plymouth.gov.uk
- Staff, children and other members of the household must wear suitable clothing.
- Staff will only use school accounts and devices for live-streaming.
- Staff will only use platforms provided or authorised by the school.
- Devices used by participants, including the member of staff, should be in appropriate areas, for example not in bedrooms; and where possible be against a neutral background.
- Language, behaviour and conduct must be appropriate, and consistent with normal school expectations, including that of any family members in the background.

- At the start of the lesson the member of staff will establish clear ground rules e.g. when and how students can speak. All participants will conform to these.

- Any poor behaviour towards the teacher or other pupils; or misuse of the system will be dealt with under the school's behaviour/discipline policy

- Parents will not interact with the member of staff during the lesson unless invited to do so by the member of staff. Any concerns will be raised with the member of staff outside the live-streamed lesson

- The member of staff will be sensitive to the needs and feelings of all children including those with SEND.

- Where a virtual lesson consists of participants at school and at home, the member of staff will ensure that appropriate control measures are in place for children in the classroom who should not appear on camera.

- Where a pupil at home should not appear on camera, his/her parents will ensure that his/her camera is turned off and any other appropriate control measures are taken.

- Pupils/parents will not share usernames, passwords or access codes with anybody else.

- Only content agreed by the teacher will be shared in the live-streamed lesson.

- Video calls should have the prior agreement of a member of SLT. Calls will only take place at a pre-arranged time. The times of video calls will be published for parents and pupils in advance

- Entry to a live-streamed lesson will only be through a link for the meeting/videocall distributed by the school. Only people invited by the member of staff are permitted to *enter* the lesson. Staff will only admit parents identified by name

- The class teacher will be the last person to leave the call and with no capacity for the children to return unsupervised

- Parents/children/third parties will not share the lesson link with anyone else

- Video calls will be recorded by the school and stored on Google Drive for six months so that the video can be reviewed if the need arises.

- Parents, children and other third parties will not record the lesson by any direct or indirect means without the permission of the teacher/member of staff leading the lesson.

- The member of staff will have control over all participants' microphones and cameras

- The member of staff will understand how to immediately end the lesson for all participants, and will do so in the event of unsuitable behaviour, language or content being shared/observed.

- The member of staff will remove any pupil from the live-streamed lesson without warning if he/she deems it to be necessary

- Safeguarding concerns will be dealt with through the school's Safeguarding Policy and procedures

I give consent for my son/daughter to participate in live-streamed lessons/meetings in accordance with the above protocols

Signed: …….. (parent) Date: …….

Pupil's name: …… Class: …….

Or for staff:

I have read and understand the above protocols for use of live-streamed lessons/meetings

Signed: …….. Date…..……..

Appendix 2

Online Safety Progression

(Based on the 8 key areas from 'Education in a connected world')

Self Image and Identity						
EYFS	KS1		Year 3 and 4		Year 5 and 6	
	Year A	Year B	Year A	Year B	Year A	Year B
Know that I can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who asks me to do something that makes me feel sad,	Know that there may be people online who could make me feel sad, embarrassed or upset. Know that if	Know and can explain how other people's identity online can be different to their identity in real life.	Know and can explain what is meant by the term 'identity'. Know and can explain how I can represent myself in	Know and can explain how my online identity can be different to the identity I present in 'real life'.	Know and can explain how identity online can be copied, modified or altered. Know and can demonstrate	Know and can describe ways in which media can shape ideas about gender. Know and can identify messages about

embarrassed or upset. Know and can explain how this could be either in real life or online	something happens that makes me feel sad, worried, uncomfortable or frightened. Know and can give examples of when and how to speak to an adult I can trust.	Know and can describe ways in which people might make themselves look different online. Know and can give examples of issues online that might make me feel sad, worried, uncomfortable or frightened; Know and can give examples of how I might get help.	different ways online. Know and can explain ways in which and why I might change my identity depending on what I am doing online (e.g. gaming; using an avatar; social media).	Know and can describe the right decisions about how I interact with others and how others perceive me.	responsible choices about my online identity, depending on context.	gender roles and make judgements based on them. Know and can challenge and explain why it is important to reject inappropriate messages about gender online. Know and can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. Know how to get help, both on and offline. Know and can explain why I should keep asking until I

						get the help I need.
Online Relationships						
EYFS	KS1		Year 3 and 4		Year 5 and 6	
	Year A	Year B	Year A	Year B	Year A	Year B
Know and can recognise some ways in which the internet can be used to communicate Know and give examples of how I (might) use technology to communicate with people I know.	Know that I can use the internet with adult support to communicate with people I know Know and can explain why it is important to be considerate and kind to people online.	Know that I can use the internet to communicate with people I don't know well (e.g. message a penpal in another school/ country) Know and can give examples of how I might use technology to communicate with others I don't know well.	Know and can describe ways people who have similar likes and interests can get together online. Know that there are technology specific forms of communication (e.g. emojis, acronyms, text speak). Know and can	Know and can explain why I can take back my trust in someone or something if I feel nervous, uncomfortable or worried. Know and can explain what it means to 'know someone' online and why this might be different from knowing someone in real	Know and can explain that there are some people I communicate with online who may want to do me or my friends harm. Know and can recognise that this is not my/our fault. Know that I can make positive contributions and be part of online	Know and can show I understand my responsibilities for the well-being of others in my online social group. Know and can explain how impulsive and rash communications online may cause problems (e.g. flaming, content produced in live

			explain some risks of communicating online with others I don't know well. Know and can explain why I should be careful who I trust online and what information I can trust them with. Know and can explain how my and other people's feelings can be hurt by what is said or written online.	life. Know and can explain what is meant by 'trusting someone online'. I can explain why this is different from 'liking someone online' Know and can describe strategies for safe and fun experiences in a range of online social environments. Know and can give examples of how to be respectful to others online.	communities. Know and can describe some of the communities in which I am involved and describe how I collaborate with others positively.	streaming). Know can demonstrate how I would support others (including those who are having difficulties) online. Know and can demonstrate ways of reporting problems online for both myself and my friends.
Online Reputation						

EYFS	KS1		Year 3 and 4		Year 5 and 6	
	Year A	Year B	Year A	Year B	Year A	Year B
Know and can identify ways that I can put information on the internet.	Know that information can stay online and could be copied. Know and can describe what information I should not put online without asking a trusted adult first.	Know and can explain how information put online about me can last for a long time. Know who to talk to if I think someone has made a mistake about putting something online.	Know that I can search for information about myself online. Know that I need to be careful before I share anything about myself or others online. Know who I should ask if I am not sure if I should put something online.	Know and can describe how others can find out information about me by looking online. Know and can explain ways that some of the information about me online could have been created, copied or shared by others.	Know that I can search for information about an individual online and create a summary report of the information I find. Know and can describe ways that information about people online can be used by others to make judgments about an individual.	Know and can explain how I am developing an online reputation which will allow other people to form an opinion of me Know and can describe some simple ways that help build a positive online reputation.
Online Bullying						

EYFS	KS1		Year 3 and 4		Year 5 and 6	
	Year A	Year B	Year A	Year B	Year A	Year B
Know that some people can be unkind online. I can say how this can make others feel.	Know and describe how to behave online in ways that do not upset others and can give examples.	Know and can give examples of bullying behaviour and how it could look online Know and can understand how bullying can make someone feel. Know how someone can/would get help about being bullied online or offline.	Know and can explain what bullying is and can describe how people may bully others. Know and can describe rules about how to behave online and how I follow them.	Know and can identify some online technologies where bullying might take place. can describe ways people can be bullied through a range of media (e.g. image, video, text, chat). Know and can explain why I need to think carefully about how content I post might affect others, their feelings and how it may	Know and can recognise when someone is upset, hurt or angry online Know and can describe how to get help for someone that is being bullied online and assess when I need to do or say something or tell someone. Know how I would report online bullying on the apps and platforms that I use.	Know how to block abusive users Know and can describe how to capture bullying content as evidence (e.g screen-grab, URL, profile) to share with others who can help me. Know and can identify a range of ways to report concerns both in school and at home about online bullying.

				affect how others feel about them (their reputation).	Know and can describe the helpline services who can support me and what I would say and do if I needed their help (e.g. Childline).	
Managing Online Information						
EYFS	KS1		Year 3 and 4		Year 5 and 6	
	Year A	Year B	Year A	Year B	Year A	Year B
Know how I can use the internet to find things out. Know and can name devices I could use to access information on the internet.	Know that I can use the internet to find things out. Know how to use simple keywords in search engines. Know and can describe and	Know how to use keywords in search engines. Know how to navigate a simple webpage to get to information I need (e.g. home, forward, back buttons; links,	Know how to use key phrases in search engines. Know and can explain what autocomplete is and how to choose the best suggestion.	Analyse information and differentiate between 'opinions', 'beliefs' and 'facts'. Know and understand what criteria have to be met	Know how to use different search technologies Evaluate digital content and can explain how I make choices from search results.	Know how to use search technologies effectively. Know and can explain how search engines work and how results are selected and ranked

Know how to find information (e.g. search engine, voice activated searching)	demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable worried or frightened.	tabs and sections). Know and can explain what voice activated searching is and how it might be used (e.g. Alexa, Google Now, Siri). Know that there are differences between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'	Know and can explain how the internet can be used to sell and buy things. Know and can explain the difference between a 'belief', an 'opinion' and a 'fact'. Know and can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites).	before something is a 'fact'. Know and can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in-app purchases, pop-ups) and can recognise some of these when they appear online. that some people I 'meet online' (e.g. through social media) may be computer programmes pretending to be real people.	Know and can explain key concepts including: data, information, fact, opinion belief, true, false, valid, reliable and evidence. Know and understand the difference between online mis-information (inaccurate information distributed by accident) and dis-information (inaccurate information deliberately distributed and intended to mislead). Know and can	Know and can demonstrate the strategies I would apply to be discerning in evaluating digital content. Know what is meant by a 'hoax' and can explain why I need to think carefully before I forward anything online Know how some online information can be opinion and can offer examples. Know and can explain how and why some

				Know and can explain why lots of people sharing the same opinions or beliefs online does not make those opinions or beliefs true.	explain what is meant by 'being sceptical'. I can give examples of when and why it is important to be 'sceptical'. Know and can explain why some information I find online may not be honest, accurate or legal. Know and can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen	people may present 'opinions' as 'facts' Know and can define the terms 'influence', 'manipulation' and 'persuasion' and explain how I might encounter these online (e.g. advertising and 'ad targeting'). Know and can demonstrate strategies to analyse and evaluate the validity of 'facts' and I can explain why using these strategies are important.

					(e.g. the sharing of misinformation either by accident or on purpose).	Know can identify, flag and report inappropriate content
Health, Well-Being and Life-Style						
EYFS	KS1		Year 3 and 4		Year 5 and 6	
	Year A	Year B	Year A	Year B	Year A	Year B
Know and can talk about rules that help keep us safe and healthy in and beyond the home when using technology	Know and can explain rules to keep us safe when we are using technology both in and beyond the home.	Know and can explain simple guidance for using technology in different environments and settings. Know and can say how those rules/guides can help me	Know why spending too much time using technology can sometimes have a negative impact on me Know and can give some examples of activities where it is easy to spend a lot of time engaged in technology (e.g.	Know how using technology can distract me from other things I might do or should be doing. Know that there are times or situations when I might need to limit the amount of time I use technology.	Know and can describe ways technology can affect healthy sleep and can describe some of the issue. Know and can describe some strategies, tips or advice to promote healthy sleep with regards to technology	Know and can describe common systems that regulate age-related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose. Know, can assess and action different

			games, films, videos).	Know and can suggest strategies to help me limit this time.		strategies to limit the impact of technology on my health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and exercise). Know and can explain the importance of self-regulating my use of technology, demonstrating the strategies I use to do this (e.g. monitoring my time online, avoiding accidents).
Privacy and Security						
EYFS	KS1		Year 3 and 4		Year 5 and 6	

	Year A	Year B	Year A	Year B	Year A	Year B
Know and can give some simple examples of my personal information (e.g. name, address, birthday, age, location). Know the people I can trust and can share my personal information with Know and can explain why I can trust them.	Know and can talk about more detailed examples of information that is personal to me (e.g. where I live, my family names, where I go to school). Know and can explain why I should always ask a trusted adult before I share any information about myself online. Know and can explain how passwords can be used to protect	Know and can describe how online information about me could be seen by others. Know, can describe and explain some rules for keeping my information private. Know what passwords are and can use passwords for my accounts and devices. Know how many devices in my home could be connected to	Know reasons why I should only share information with people I choose to and can trust. Know that if I am not sure or I feel pressured, I should ask a trusted adult. Know, understand and can give reasons why passwords are important. Know some simple strategies for creating and keeping	Know what a strong password is Know some strategies for keeping my personal information private, depending on context. Know that others online can pretend to be me or other people, including my friends and can suggest reasons why they might do this. Know how internet use can be monitored.	Know how to create and use strong and secure passwords Know how many free apps or services may read and share my private information (e.g. friends, contacts, likes, images, videos, voice, messages, geolocation) with others. Know how and why some apps may request or take payment for additional content (e.g. in-app purchases)	Know why I need to use different passwords for a range of online services. Know effective strategies for managing passwords (e.g. password managers, acronyms, stories). Know what to do if my password is lost or stolen. Know what app permissions are and can give some examples from the technology or

	information and devices.	the internet and can list some of those devices.	passwords private Know how connected devices can collect and share my information with others.		and explain why I should seek permission from a trusted adult before purchasing.	services I use. Know simple ways to increase privacy on apps and services that provide privacy settings. Know ways in which some online content targets people to gain money or information illegally; can describe strategies to help me identify such content (e.g. scams, phishing).
Copyright and Ownership						
EYFS	KS1		Year 3 and 4		Year 5 and 6	

	Year A	Year B	Year A	Year B	Year A	Year B
Know that work I create belongs to me. Know that I can name my work so that others know it belongs to me.	Know why work I create using technology belongs to me Know that my work belongs to me (e.g. 'it is my idea' or 'I designed it'). Know how to save my work so that others know it belongs to me (e.g. filename, name on content).	Know and can describe why other people's work belongs to them. Know that that content on the internet may belong to other people.	Know why copying someone else's work from the internet without permission can cause problems. Know and can give examples of problems related to permission online	Know that when searching on the internet for content to use why I need to consider who owns it and whether I have the right to reuse it. Know and can give some examples of why I need to consider who owns digital content	Know, can assess and justify when it is acceptable to use the work of others. Know and can give some examples of content that is permitted to be reused.	Know how to demonstrate the use of search tools to find and access online content which can be reused by others. Know how to make references to and acknowledge sources I have used from the internet

Suggested Resources:

https://projectevolve.co.uk/toolkit/

https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/teaching-resources

https://www.childnet.com/parents-and-carers/hot-topics/critical-thinking

https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials

https://www.commonsense.org/education/