St. Hubert's Roman Catholic Primary School

Hallfield Road, Great Harwood, Blackburn Tel: 01254 885778
Headteacher: Mrs J. M. Brooks

Online Safety Policy 2024-2025

Created by: Megan Rawlinson-White
Reviewed by: Governing Body
Review Date: September 2025

Believe to Achieve: Love God, Love Learning, Love One Another

Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people: Miss M Rawlinson-White (Online Safety Campion and Computing Subject Leader) and Mrs J Brooks (Headteacher and DSL).

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created – Date: September 2024

The implementation of this policy will be monitored by Miss M Rawlinson-White and Mrs J Brooks.

This policy will be reviewed as appropriate by Miss M Rawlinson-White and Mrs J Brooks.

Approved by ..... (Headteacher)

Date .....

Approved by ..... (Governor)

Date .....

Contents

Developing and Reviewing this Policy.....2

Contents.....3

1. Introduction.....4

2. St Hubert's vision for Online Safety.....4

3. The role of St Hubert's Online Safety Champion.....5

4. Policies and practices.....6

4.1 Security and data management..... 6

4.2 Use of mobile devices..... 7

4.3 Use of digital media 8

4.4 Communication technologies..... 9

4.5 Acceptable Use Policy (AUP)..... 15

4.6 Dealing with incidents 15

5. Infrastructure and technology..... 16

6. Education and Training..... 19

6.1Online Safety across the curriculum..... 19

6.2 Online Safety – Raising staff awareness..... 20

6.3Online Safety – Raising parents/carers awareness 20

6.4Online Safety – Raising Governors' awareness..... 21

7. Standards and inspection 21

Appendix 1 – AUP KS1..... 22

Appendix 2 – AUP KS2 23

Appendix 3 – AUP Parents/Carers 26

Appendix 4 – AUP SEN Pupils 30

Appendix 5 - AUP Staff, Governors and Volunteers 34

1. Introduction

This policy applies to all members of the St Hubert's community, including staff, pupils, parents/carers, visitors and school community users. Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure that our school community are prepared to deal with the safety challenges that the use of technology brings.

The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Vision for Online Safety

St Hubert's RC Primary School aims to provide a diverse, balanced and relevant approach to the use of technology where the children have the opportunity to learn in an environment where security measures are balanced appropriately in order for children to be able to learn effectively. We aim to equip the children with the skills and knowledge to use technology appropriately and raise awareness of the risks of technology both inside and outside the school community. We feel it is essential that children have strategies to deal with these risks. As a school we recognise the need for an effective e-safety policy.

3. The role of the school's Online Safety Champion

The Online Safety Champion for St Hubert's RC Primary School is Miss M Rawlinson-White.

The role of the Online Safety Champion in our school includes:

▪ To have operational responsibility for ensuring the development, maintenance and review of the schools Online Safety Policy and associated documents, including Acceptable Use Policies.

▪ Ensure that the policy is implemented and that compliance with the policy is actively monitored.

▪ Ensure all staff are aware of our reporting procedures and requirements, should an Online Safety incident occur.

▪ Keeping personally up to date with Online Safety issues and guidance through liaison with the Lancashire County Council Schools ICT Team and through advice given by national agencies such as the Child Exploitation, Child Net and Online Protection Centre (CEOP).

▪ Providing or arranging Online Safety advice/training for staff, parents/carers and governors.

▪ Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.

▪ Liaising closely with the school's Designated Senior Person for E safety J. Brooks (Head Teacher).

▪ DSL to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and Practices

Our Online Safety policy should be read in conjunction with the following other related policies and documents:

- St Hubert's Child Protection and Safeguarding Policy
- Mobile Phone Policy
- AUP Policy (Page 15)
- EVC Policy

4.1 Security and Data Management In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data must be:

- Accurate
- Secure
- Fairly and lawfully processed.
- Processed for limited purposes.
- Processed in accordance with the data subject's rights.
- Adequate, relevant and not excessive.
- Kept no longer than is necessary.
- Only transferred to others with adequate protection.

At St Hubert's, data is kept secure, and all staff are informed as to what they can/cannot do with regard to data in the following ways: Within school there are 2 different networks – administration and curriculum.

Admin network –

- Password protected at the appropriate level for the necessary members of staff to access.
- Passwords regularly changed.

▪ Within access to the computer programs password protected again at the most appropriate level to the seniority of the staff.

▪ Data transferred securely to other schools.

Curriculum network –

▪ Curriculum computers managed by a domain server.

▪ All staff have individual log ins to access the computer which allow access only to their personal folder and folders with shared access.

▪ Class log in which enable children to save in their class folder but prevent children from changing settings within control panel.

▪ Administrators log in – Access by technician (Mr Rawat), bursar (Mrs Fox) and the Head Teacher (Mrs Brooks) only.

4.2 Use of mobile devices

At St Hubert's we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

▪ School Laptops need to be signed for when allocated to a member of staff and returned to school when the member of staff leaves/changes position.

▪ All school laptops will be set up in the same way by the ICT Technician, Mr Rawat.

▪ Any software required by the member of staff will be installed by the ICT technician, Mr Rawat.

▪ No other additional software should be installed unless permission is given by SLT.

▪ Any problems/errors with a laptop and it should be returned to school and ticketed to the ICT technician.

▪ Laptops may not be used for personal access to Social Networking, Chat Rooms or instant messaging.

▪ Use of laptops at home follow the same conditions as internet usage in school.

Cameras

To protect all staff no personal cameras or cameras on mobile phones should be used in school or on educational visits to take photos of children.

All pictures on school cameras / Ipads should be downloaded onto the school network.

School laptops/ tablets

Any digital equipment must be signed out in a book kept in the office and the rules above apply.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.

At St Hubert's we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

▪ The school seeks consent from parents/carers as to whether their child may appear in the media.

▪ A list of children whose photo must not appear on the school website is circulated among staff.

▪ Parental/Carers permission is obtained.

▪ Images of pupils who have left the establishment may be kept on the school server but are not used in any publications beyond a year after they have left.

▪ Staff are aware that full names and personal details will not be used in any digital media and particularly in association with photographs.

▪ Parents and Carers are not allowed to take photographs/videos at events.

▪ It is made clear to all staff that photographs and videos are only taken using school equipment, the children are appropriately dressed and then are only downloaded onto the school network where only authorised users can log on and access.

▪ Parents and Carers are directed to online safety sites where the dangers of publishing images and videos of pupils or adults on social network or websites without the consent of the person involved is clearly explained.

4.4 Communication technologies

At St Hubert's the following statements reflect our practice in the use of email.

Email

The government encourages the use of e-mail as an essential means of communication. Direct emails can bring significant educational benefits however the following points need to be addressed.

Staff

▪ All users have access to the Lancashire Grid for Learning service as the preferred school email system.

▪ Only official email addresses should be used to contact staff.

▪ The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts.

▪ Any incidents of SPAM should be reported to the Westfield Centre.

▪ All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

▪ All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

▪ All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

▪ All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks:

These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. Therefore, staff and children are unable to access through the school network. The latest document 'Keeping children safe in education' is available to view - Keeping children safe in education.

Lancashire County Council Guidance relating to the use of social networking sites is as follows: Where information can easily reach a wider audience than might have originally been intended, in certain circumstances, the conduct of the employee might also be deemed to have damaged the reputation of the school and the trust and confidence in the school that parents and the community can reasonably expect. Therefore, the authority's advice to staff is that they should be very careful in how they communicate with pupils via the use of technology and in terms of what they elect to share about themselves through internet-based networking sites such as Facebook and Twitter. In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

The main points being –

▪ Staff should not give their personal contact details to children or young people, including their mobile number, details of any blogs or personal website.

▪ Internet or web-based communication channels should not be used to send personal messages to a child/young person.

▪ Social networking sites are not to be used by children or adults within school.

▪ Ensure that if a social networking site is used outside of the workplace, details are not shared with children and young people and privacy settings are set at maximum.

▪ Laptop and other handheld devices which are borrowed or loaned out to members of staff should not be used to access social networking sites for a personal nature.

▪ Inappropriate comments about the workplace are not posted.

▪ Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.

▪ Pupils must not be added as "friends" on any Social Network site.

▪ Twitter may be accessed on the admin network and must only accessed by Headteacher, SLT, DSL for online safety or the Online Safety Champion.

At St Hubert's, staff may use Class Dojo as a means of sharing and communicating information with parents. This function is only to be used by staff in school. No pictures of children should be shared from Class Dojo and messages should be kept professional. If picture(s) of children's work is shared, staff should ensure that the work is anonymous to protect the child and his/her identity. See our communications policy for further information.

Mobile

Mobile phone use and ownership by young people is growing. St Hubert's does not permit children to have mobiles in school without written permission and they should be switched off at all times and locked away by a staff member. The following risks are made clear to pupils when using mobiles outside of school –

▪ Exposure to inappropriate material

▪ Physical danger

▪ Cyberbullying

▪ Legal, financial and commercial considerations (ref Becta Signposts to safety)

Staff are made aware of the risks of unfiltered internet content when accessing through a mobile phone and the apps which can access personal details on phones.

At St Hubert's the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

Staff

- Keep personal phone numbers private and personal mobile phones should not be given to parents.

- Personal mobiles should not be used to contact pupils or parents, except in an emergency when the mobile number needs to be withheld.

- Pictures and videos are not to be taken using personal mobile phones, on the school premises.

Instant Messaging

At St Hubert's, the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

▪ The use of Instant messaging (e.g. MSN messenger) is not permitted.

▪ Use of social-networking websites (e.g. Twitter, MySpace, Facebook, Instagram, Piczo, etc.) is not permitted.

▪ Children and staff must not access public or unregulated chat rooms.

▪ Children may access web-based games/activities. This may involve playing against users from other schools but should not extend to communication with other users.

Instant Messaging is only appropriate in school when part of a Video Conferencing session through Zoom where images are transmitted through a webcam through a secure link.

Sexting

Sexting can be defined as the activity of sending text messages that are about sex or intended to sexually excite someone. This is not appropriate

for school and any instance of this between children will be treated as an online safety/child protection incident and will be dealt with by the Online Safety Champion (Miss Rawlinson-White) and Child Protection Lead (Mrs Brooks) in school.

Web sites and other online publications

Content of School Website-

▪ Publication of information on a website should be considered from a security point of view.

▪ The point of content on the web site should be the school address, school e-mail and telephone number.

▪ Staff or pupils' home information will not be published.

▪ Web site photographs that include pupils will be selected carefully and will only be used if parents have given permission.

▪ Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.

▪ The website should be subject to frequent checks to ensure that no material has been inadvertently posted, which may put children or staff at risk.

▪ Copyright and intellectual property rights must be respected.

▪ When photographs to be used on the website are saved, names of individuals should not be used as file names. Importance of the Internet and benefits to education.

▪ The purpose of the Internet is to raise educational standards to promote pupil achievement, to support professional work of staff and to enhance the school's management information and business administration system.

▪ Access to world-wide educational resources including museums and art galleries.

▪ Educational and cultural exchanges between pupils world-wide.

▪ Staff professional development through access to national developments educational material and good curriculum practice.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

At St Hubert's the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

▪ Staff and pupils are not allowed to download programs from the Internet or via e-mail programs such as Hotmail onto school computers without permission from the ICT SL /Technical support officer.

▪ Emerging technologies will be examined for educational benefit and downloaded if they are seen to be appropriate for educational use by the Computing Subject Leader or technician.

Video conferencing

Video Conferencing is a valuable tool bringing the outside world into the classroom.

At St Hubert's the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing: Parents' carers will have signed a consent form enabling their child to participate in video conferencing sessions.

▪ Headteacher to approve video conferencing sessions. All session times should be logged including the date, time and name of the external organisations taking part.

▪ Pupils using video conferencing equipment should be supervised at all times.

▪ All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.

▪ Copyright, privacy and Intellectual property Rights IPR legislation will be breached if images, video or sound are recorded without permission.

▪ Check whether recordings are repurposed in any other form or media other than the purpose originally agreed.

4.5 Acceptable Use Policy (AUP)

St Hubert's use Acceptable Use Policies (AUPs) to ensure that all users stay safe whilst using the internet and other communication technologies. These policies reflect the technologies, procedures and practice within our school.

See Appendix for:

A1 – Acceptable Use Policies KS1 (Page 22)

A2 – Acceptable Use Policies KS2 (Pages 23-25)

A3 – Acceptable Use Policies Parents (Pages 26-28)

A4 - Acceptable Use Policies SEN Pupils (Pages 30-33)

A5 – Acceptable Use Policies Staff, Governors and Volunteers (Pages 34-38)

4.6 Dealing with incidents

All incidents should be recorded on CPOMS. This must be audited on a regular basis by the Headteacher (Mrs Brooks) and the Online Safety Champion (Miss Rawlinson-White).

Illegal offence

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) . They are licensed to investigate – schools are not!

Examples of illegal offences are:

▪ Accessing child sexual abuse images

▪ Accessing non-photographic child sexual abuse images

▪ Accessing criminally obscene adult content

▪ Incitement to racial hatred More details regarding these categories can be found on the NSPCC website, Types of abuse.

Online Safety Incidents

▪ The Headteacher (Mrs Brooks) and the Online Safety Champion (Miss Rawlinson-White) are responsible for dealing with Online Safety incidents.

▪ All staff are aware of the types of Online Safety incidents and how to respond appropriately. E.g. illegal or inappropriate.

- Children are informed of procedures during Online Safety sessions.
- Incidents are always logged on CPOMS.
- Incidents are logged by one of the named people dealing with the incident (Online Safety Champion, Headteacher)
- Appropriate measures are put in place to respond to incidents and prevent a recurrence of an incident.
- Parents and external agencies are informed as appropriate.

5. Infrastructure and technology

St Hubert's RC Primary School subscribes to BT Lancashire Education Service. Lightspeed provides internet content filtering. The filtering service offers a high level of protection, but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription and is installed on all computers and configured to receive regular updates. Any virus alerts are e-mailed to bursar@sthuberts.org.uk

Pupil Access:

▪ Pupils log on to the network using their class username and password.

▪ Pupils are supervised when using the internet or other online materials.

Passwords:

▪ Staff are aware of the guidelines in the Lancashire ICT Security Framework

▪ All users of the school network have a secure username and password. The level of access and permission is appropriate to their status.

▪ The administrator password is known by the SLT, Online Safety Champion and the school technician. A copy is kept in an envelope in the school safe.

▪ Through online safety lessons children are reminded of the importance of keeping passwords secure.

▪ Children's passwords are changed annually. Office admin network passwords are changed every year.

Software/hardware:

▪ St Hubert's has legal ownership of all software.

▪ Software is appropriately licenced, and a file of licences are kept in the ICT storeroom.

▪ Equipment and software is audited. Equipment is recorded in the school record log which is on the protected server. All staff have a list of software on computers.

▪ The Online Safety Champion and technician control what software is installed on the schools' systems.

▪ St Hubert's have purchased and manage licenses for the software used online.

Managing the network and technical support:

▪ Servers, wireless systems and cabling is securely located and physical access is restricted.

▪ All wireless devices go through the school's proxy server.

▪ Wireless devices are only accessible through a secure password.

▪ The ICT technician is responsible for managing the security of the school network.

▪ Safety and Security of the school network is reviewed annually or more frequently if issues occur.

▪ Group policies are distributed from the server to keep children safe.

▪ Computers and laptops are kept up to date with updates and patches rolled out from the server.

▪ The ICT Technician periodically ensures updates have taken place.

▪ Staff and pupils are required to log or lock out of a computer when left unattended.

▪ Only the administrator is allowed to download executable files or install software.

▪ Breaches or security or suspicion of breaches of security are reported to the Online Safety Champion and recorded in a folder in office.

▪ Removable storage devices may be used by school staff and visitors as long as they use SOPHOS to scan device before opening folders.

▪ External technical support providers are aware of the schools' requirements and standards regarding e-safety.

▪ The Computing Subject Leader and Online Safety Champion is responsible for liaising with technical support staff.

Filtering and virus protection:

▪ Staff report websites which need blocking or unblocking to Online Safety Champion

▪ Staff report suspected or actual computer virus to Online Safety Champion

▪ School laptops automatically update antivirus protection when connected to the internet.

6. Education and Training

6.1 Online Safety across the curriculum

Acceptable access to the Internet.

It is necessary to develop good practice when accessing the Internet and develop it as a tool for teaching and learning. The quantity of information needs to be cut down by guiding pupils to appropriate web sites rather than suggesting use of the whole Web.

▪ The school Internet access will be filtered with a service known as Smart Filter.

▪ Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.

▪ Children will be taught the principles of effective searching as part of their core digital literacy skills development.

▪ Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

▪ Planned unit of Online Safety is taught in each year group and linked to other subjects where appropriate. Within this, children are made aware of the relevant legislation when using the internet (appropriate to age group) e.g. data protection Act 1998 and copyright implications. Children are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

▪ This unit also covers cyberbullying and the impact it can have. PSHE is used to address any issues throughout the year and children are provided with strategies and points of contact if they need help.

▪ There is an additional focus on E Safety during the National Online Safety Awareness Week Online Safety education is differentiated for pupils with SEN by using the most appropriate materials to meet their needs.

▪ Children are taught to critically evaluate materials and sources of information on the internet so research skills can be used effectively across the curriculum.

▪ Children are taught about the need to stay safe at school and how to stay responsible outside school.

6.2 Online Safety – Raising staff awareness

▪ Online Safety Champion has received recent Online Safety training.

▪ All staff are expected to promote and model responsible use of ICT and digital resources.

▪ The safety policy is discussed with all new staff to ensure they understand the content and the procedures in place.

▪ Updates on the Online Safety policy are discussed at staff meetings.

6.3 Online Safety – Raising parents/carers awareness

"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." (Byron Report, 2008).

▪ School newsletters and website provide information on the benefits and risks of using various technologies.

▪ School promotes external e-safety resources and online materials.

▪ School uses Dojo and Twitter to communicate with parents and raise awareness of Online Safety.

6.4 Online Safety – Raising Governors' awareness

Governors are kept up to date through reports at governor meetings and through a governor with specific responsibilities for ICT.

The Online Safety policy is reviewed by the governing body.

7. Standards and inspection

The children will be knowledgeable about how to stay safe online and understand who to talk/report to if there is a problem. Parents are aware of where to get support and the dangers their children face in a digital world and measures; they can put in place to reduce the risks.

E-Safety incidents are recorded by staff and monitored by the Headteacher (Mrs Brooks) and the Online Safety Champion (Miss Rawlinson-White). Policies and procedures are reviewed in light of any incidents. In the event of a serious incident, schools should contact **Lancashire's Schools Safeguarding Officer on 01772 531196.**

Any incidents are recorded are monitored to see if there is any recurring pattern or whether they are a one off.

Staff recognise the importance of staying safe online and model this.

AUP's are reviewed annually with the Online Safety policy reviewed biannually.

Appendix 1 – AUP KS1

St Hubert's RC Primary School

Acceptable Use Policy (AUP) for

KS1 PUPILS

LGfL DigiSafe

My name is _____

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

My trusted adults are:

_____ **at school**

_____ **at home**

For parents/carers

To find out more about online safety, you can read St Hubert's full Online Safety Policy found on our website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). You can find support and online safety resources for parents at https://www.lancashire.gov.uk/youthzone/need-to-know/online-safety/

Appendix 2 – AUP KS2

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
KS2 PUPILS

DigiSafe

LGfL

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

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
KS2 PUPILS

12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
KS2 PUPILS

22. *I am a researcher online* – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

For parents/carers

If your parents/carers want to find out more, they can read St Hubert's full Online Safety Policy found on our website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). They will also have been asked to sign an AUP for parents.

~~~~~~~~~~~~~~~~~~ ✂ ~~~~~~~~~~~~~~~~

I have read and understood this AUP Agreement.

If I have any questions, I will speak to a trusted adult: at school that includes _____.

Outside school, my trusted adult is _____.

Name: _____

Date: _____

Year group:_____
~~~~~~~~~~~~~~~~~~

Appendix 3 – AUP Parents/Carers

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for PARENTS

DigiSafe

LGfL

What is an AUP?

We ask all children, young people and adults involved in the life of St Hubert's R.C. Primary School to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). Your child has also signed an AUP in school. This was explained and read though by the class teacher.

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read St Hubert's full Online Safety Policy found on our website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Miss Fitzpatrick on g.fitzpatrick@sthuberts.org.uk.

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
PARENTS

DigiSafe

LGfL

What am I agreeing to?

1. I understand that St Hubert's R.C. Primary uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides

guides to help parents do this easily for all the main internet service providers in the UK.

9. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
10. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which has been sent home and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
11. I can find out more about online safety at St Hubert's by reading the full Online Safety Policy found on their website and can talk to their class teacher or a member of the SLT if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

Please note that parents may also be interested in the school's approach to the following matters, which are all covered as sections within the overall school Online Safety Policy:

- Roles and responsibilities of members of the school community
- Education and curriculum
- Handling online-safety concerns and incidents
- Actions where there are concerns about a child
  - Sexting and upskirting
  - Bullying
  - Sexual violence and harassment
  - Misuse of school technology (devices, systems, networks or platforms)
  - Social media incidents
- Data protection and data security
- Appropriate filtering and monitoring
- Electronic communications
- Email
- School website
- Cloud platforms
- Digital images and video
- Social media
- Device usage

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
PARENTS

Please return this slip to St Hubert's School once completed.

I/we have read, understood and agreed to this policy.

Signature/s: _____

_____

_____

Name/s of parent / guardian: _____

_____

_____

Date: _____

Appendix 4 – AUP SEN Pupils

IncludED

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
SEN PUPILS

DigiSafe
LGfL

What I Must do to Keep Safe Online and With Devices

Online means anything connected to the internet. Most devices and apps are connected to the internet.

IncludED

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
SEN PUPILS

DigiSafe
LGfL

Devices are technology like: computers, laptops, games consoles, tablets and smart phones.

I will only use the devices I am allowed to use.

I will ask a trusted adult before I use new websites, games or apps.

IncludED

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
SEN PUPILS

DigiSafe
LGfL

✓ I will ask for help if I'm stuck or not sure.

✓ I will be kind and polite to everyone online.

✓ I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.

IncludED

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
SEN PUPILS

DigiSafe
LGfL

✓ I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.

✓ I will tell a trusted adult if I feel bad or unsafe when I am using a device.

I know people online sometimes tell lies.

IncludED

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
SEN PUPILS

DigiSafe
LGfL

They might lie about who they are or where they live.

I never have to keep secrets from my trusted adults.

I will not change clothes or undress in front of a webcam.

I will always ask a trusted adult before telling anyone my private

IncludED

St Hubert's RC Primary School
Acceptable Use Policy (AUP) for
SEN PUPILS

DigiSafe
LGfL

information or location.

I know that anything I do or say online might stay there forever.

It can be given to my family, my friends or strangers.

This could make me feel sad or embarrassed.

IncludED

DigiSafe

LGfL

St Hubert's RC Primary School

Acceptable Use Policy (AUP) for

SEN PUPILS

My trusted adults are _____ at school

My trusted adults are _____ at home

My name is _____

Appendix 4 – AUP Staff, Governors and Volunteers

ST. HUBERT'S R. C.
PRIMARY SCHOOL

St. Hubert's Roman Catholic Primary School

Hallfield Road, Great Harwood, Blackburn Tel: 01254 885778
Headteacher: Mrs J. M. Brooks

Acceptable Use Policy for Staff, Governors and Volunteers. (AUP)

Created by: Megan Rawlinson-White
Reviewed by: Governing Body
Adopted by Governors: Sept 2024
Review Date: Sept 2025

Believe to Achieve: Love God, Love Learning, Love One Another

What is an AUP?

We ask all children, young people and adults involved in the life of St Hubert's R.C. Primary School to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and you will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have legal / professional obligations, and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy. See School Website.

Where can I find out more?

All staff, governors and volunteers should read St Hubert's full Online Safety Policy located on our website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Miss Rawlinson / m.rawlinson@sthuberts.org.uk

Believe to Achieve: Love God, Love Learning, Love One Another

What am I agreeing to?

1. I have read and understood St Hubert's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult) Mrs J Brooks and Mr C Barnacle.
3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
   - not sharing other's images or details without permission
   - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in St Hubert's Online Safety policy - social media guidance.
9. I agree to always adhere to all provisions of the school Data Protection Policy, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify Miss M Rawlinson if I suspect a breach.

Believe to Achieve: Love God, Love Learning, Love One Another

10. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
11. I will use school devices and networks/internet/platforms/other technologies for school business, and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
12. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
13. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
14. I will follow the guidance in the Online Safety Policy for reporting incidents – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, up skirting, bullying, sexual violence and harassment, misuse of technology and social media.
15. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Believe to Achieve: Love God, Love Learning, Love One Another

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

Believe to Achieve: Love God, Love Learning, Love One Another