

ST ALBAN'S R.C. PRIMARY SCHOOL



Online Safety Policy

1. Authorised by: _____
(Headteacher)

Date: _____

2. Authorised by: Edmund A. Baker
(Chair of Governors)

Date: 15th March 2023.

Date of issue: Spring Term 2023

Review Date: Spring Term 2025

ST. ALBAN'S ROMAN CATHOLIC SCHOOL MISSION TATEMENT

In the light of Jesus we love together, hope together and learn together.



We are a learning community where **EVERY** person is supported to aspire, achieve and succeed following the teachings of Christ. Recognising that we are all made in the image and likeness of God we **WELCOME** all to our community.

In an inclusive, safe and secure environment where hard work, achievements and talents are recognised and celebrated we ensure the **WELFARE** of all.

We place the **WORD** God at the centre of all we do, listening to, telling and being part of the story of Jesus Christ.

In **WORSHIP** we foster and deepen our relationship with God through our actions, thoughts and words, rooted in the sacramental life of the church.

Showing **WITNESS** to a loving God who is at the heart of all we do, we develop active citizens who live out the Gospel values now and in the future.

Online safety POLICY

Using new learning technologies effectively and safely

Our Online safety Policy has been written by the school, building on the Blackburn with Darwen policy: "BLACKBURN WITH DARWEN LOCAL SAFEGUARDING CHILDREN BOARD: E-SAFETY POLICY AND GUIDANCE", as a result of the Every Child Matters agenda set out by the Government (Education Act 2002 and the Children Act 2004).

https://panlancashirescb.proceduresonline.com/pdfs/e_safety_policy_and_guidance.pdf

It has been agreed by the senior leadership team and approved by Governors. It will be reviewed after 2 years.

The online safety Policy relates to other policies including those for Computing, bullying and for child protection.

- The online safety policy and its implementation will be reviewed after 2 years or in response to an incident.
- All staff will be given the school online safety policy and its importance explained.
- Parents' attention will be drawn to the school online safety policy in newsletters and on the school website.
- Evaluation of the effectiveness of the policy is undertaken through:
 - Parent surveys- annual
 - Pupil surveys- annual
 - Assessment of pupils online safety knowledge
 - Staff feedback

Responsibility for Online safety

At St Alban's RC Primary School we believe that all staff have a responsibility for online safety within our school.

The online safety policy relates to other curriculum policies including Computing, anti bullying and safeguarding. The Safeguarding lead is Diana Boardman. This role includes leading on online safety.

Online safety Education

Why Internet and communication technology use is important

'Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age...' OFSTED 2013.

"One of the barriers to pupils developing knowledge was the belief they are "digital natives" and already experts. But "for pupils to use computing devices effectively, they need to be taught how to use them". OFSTED 2022

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Pupils

As the children's access and understanding expands, so should the guidance and rules to ensure safe access and use of the internet and communication technology.

The LA's filtering system (Talk straight) minimises the risk of pupils accessing undesirable content, however the school believes it is important to educate children in how to stay safe inside and outside of school and provide opportunities to learn how to assess and manage risk for themselves..

A progressive online safety curriculum is taught to each year group; alongside our Teach Computing scheme of work, online safety lessons are enriched by units from Project Evolve- "*a free digital literacy toolkit that supports the safe online development in children and young people.*" Online safety will also be taught in part via a rich and carefully considered PSHE curriculum. Cross-curricular opportunities to promote online safety will be taken by teaching staff in all other day to day learning.

Online safety education in school will be appropriate to the children's age and experience and will cover the following:

- Evaluating Internet content.
- Developing an understanding of copyright law.
- Using technology responsibly (pupils will be given clear objectives for use of the internet and communication technology).
- Using the Internet effectively for research, communication and sharing ideas.
- Developing an understanding of accuracy and bias
- Developing an understanding of the effects that viruses etc. can have on a computer and how to protect computers from them.
- Keeping information private.
- Communicating effectively including understanding cyber bullying and stranger danger.
- Presenting themselves and others appropriately.
- Respecting the privacy of others.
- Knowing what to do if they feel uncomfortable or worried by something they have seen or done using technology.

Keeping Pupils Safe

In order to keep our pupils safe:

- All pupils will sign an acceptable use policy appropriate to their age that is linked to the school rules
- Online safety rules will be displayed around the school and specifically near areas where computers and other devices are frequently used.
- Staff and pupils will be encouraged to refer to these rules regularly.
- Pupils may only use approved digital methods of communication on the school system and they will be educated about how to stay safe before using them.
- Pupils will be taught to use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils will be taught about the dangers of radicalisation and extremism at an appropriate level for their age
- Online safety will be promoted whenever possible- cross-curriculum. Online safety will be covered in our PSHE curriculum as well as computing.

Inappropriate use/behaviour

Sanctions for inappropriate use of the internet will be clear and appropriate to the age of the children and the type of behaviour. Children and staff will be made aware of what is and is not acceptable when using school technology. A record of online safety concerns will be available via CPOMS. Children should be taught:

- To keep their logons private
- Not to attempt to use another user's login details
- To access only those sites permitted by the supervising member of staff
- To inform an adult should they have any concerns or worries about using technology
- To use reporting tools (such as CEOP button, Hector, Childline, NSPCC) and minimise screen immediately if they see something online which makes them feel uncomfortable.
- To seek help from a teacher if they see something which makes them feel uncomfortable.
- Be polite and respectful at all times when using online communications
- Not to click on any link or download software without permission

Parents

Children often seem more at home in the digital world than their parents. To ensure that children are the safest they possibly can be, we must educate parents about the risk of using the internet and communication technology for their children and the potential for their own use of technology to place themselves or their child at risk.

We ensure parents receive information and training by:

- Providing links to information and resources for parents on our school website and text service
- Providing regular updates to parents through newsletters (E.g. National Online Safety guides- tailored to current issues)
- Inviting parents to online safety assemblies
- Providing online safety information during events such as parents evenings
- Encouraging parents to act as role models when using technology

The school will share with parents and children, our belief that:

- The unsupervised use of social network spaces intended for adults outside school is inappropriate for pupils of primary age.
- Family friendly filtering can help to keep children safe, however education and the opportunity to develop safe practice is essential for keeping children safe
- Pupils who use the internet and other communication technology may be at risk of being groomed or radicalised. It is important that parents understand that secrecy is a possible factor in both of these.
- What pupils do online now, can affect their future life.
- If a child is happy to tell a parent or carer when they are worried, they are the safest they can possibly be; therefore we encourage parents to nurture a sense of trust between them and their child when talking about using technology.

There are some excellent online tools for reporting concerns, such as the Report Abuse button which can be found on the <https://www.thinkuknow.co.uk/> site and Childline <http://www.childline.org.uk>.

Children are also encouraged to report their concerns via a member of staff or trusted adult.

Staff and the wider school community

- We ensure that all new staff receive online safety training as part of their induction
- All school staff have access to online safety materials via the school server

Materials to include:

- Online safety issues for pupils
- Reporting procedures
- Guidance on appropriate use of communication technology by staff and pupils
- Guidance for staff on how to stay safe
- Expectations in terms of passwords and data security

- Expectations in terms of professional conduct including the use of social media
- Teaching pupils to minimise the screen if they see something that makes them feel uncomfortable.

Keeping staff and pupils safe in school

- The school will work with the LA, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the IT technician and/or DSL lead who will inform the LA where appropriate so that they can take appropriate action.
- All users will be taught how to care for devices in terms of health and safety. This includes avoiding placing food or liquids near to electrical devices, carrying equipment and rules around charging and electrical sockets.
- The school internet access is designed expressly for pupil use and includes appropriate filtering.
- Sanctions for inappropriate use of the internet and communication technology are followed. A record of any misuse is kept by DSL on CPOMS.
- School staff do not use their own personal devices/accounts to contact parents and pupils. To protect staff and pupils, the school provides school email addresses. Cameras are provided for recording school related activities. Images of children should not be stored on personal devices.
- The Head teacher receives a report from the LA weekly on any issues around unsafe access.

Reporting online safety concerns

- Children are encouraged to report their concerns via a member of staff. We also encourage the children to use national resources such as ChildLine, NSPCC and CEOP.
- A record of online safety incidents will be reported to DSL via CPOMS.
- The nature of the incident and action taken are recorded with any consequences e.g. additional online safety input; discussion with parents restricting access etc.. This includes access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures.

Acceptable use agreements

- A home school agreement concerning access to the internet and communication technology will be signed by pupils in KS2 and parents in KS1/Reception (see appendix). This will be available for staff to check in the main office under personal folders
- Acceptable use agreement for school staff will be signed and kept in staff personal folders (see appendix)

Published Content

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (This may be through education and guidance, as directly reading everything is impractical)

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner. (In the Foundation Stage this may not be practical when capturing a child in the process of learning, however should be modelled as often as possible.)
- Pupils' full names will not be used anywhere, particularly in association with photographs. (some schools may wish to use first names, where there is no photograph, but staff should be aware of the risks associated with this and take appropriate precautions)
- Permission forms from parents or carers are obtained before photographs or video of pupils are published. These forms are kept in the main office in children's personal folders.
- Where pupil's work is published, the school will ensure that the child's identity is protected.
- Where school events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip

Policy Decisions

Authorising Internet access

- All staff, teaching students, visitors and governors must read and sign the 'Responsible ICT Use Agreement' (see appendix) before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access in their personal folders. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form.

Parents using still or video cameras at school

- In line with the Information Commissioner's Office, the school allows parents to record video and images during performances for person use only. We advise parents of this before each event.

Guidance for taking photographs and video during school performances and assemblies.

Information Commissioner's Office:

<https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/taking-photographs-data-protection-advice-for-schools/#:~:text=Data%20protection%20doesn't%20cover,always%20appropriate%20to%20allow%20photographs.>

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered and shared with staff before they are used in school.

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- New parents with children starting at school will be asked to sign and return a consent form for their children to access the internet (see personal folders).

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the online safety co-ordinator, the DSL via CPOMS and to the LA where necessary.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with the headteacher/a senior member of staff, who will inform the LA where appropriate.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure on request.

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where pupils may access the internet and discussed with the pupils at the start of each year. Where possible images and symbols will be used to help make them accessible to young children.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Introducing the policy to parents

Parents' attention will be drawn to the School online safety Policy and practice:

- In newsletters
- On the school website
- Via text service

Staff and the online safety policy

- All staff will be given the School online safety Policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Appendix 1 Acceptable use policy



St Alban's RC Primary School

EYFS/KS1

ICT Acceptable Use Policy (AUP)

Children

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher/an adult immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken.

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and my child: agrees to follow the Online Safety rules and to support the safe use of ICT at St Alban's RC Primary School

Parent /Carer Name (Print)

Parent /Carer (Signature)

Class Date.....

This AUP must be signed and returned before any access to school systems is allowed.



St Alban's RC Primary School

KS2
Children

ICT Acceptable Use Policy (AUP)

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers/staff read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher/an adult immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken.

Child's Signature

We have discussed this Acceptable Use Policy in school and agrees to follow the online Safety rules and to support the safe use of ICT at St Alban's RC Primary School

Name (Print)

(Signature)

Class Date.....

This AUP must be signed and returned before any access to school systems is allowed.



St Alban's RC Primary School

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources**, software, communication tools, **equipment and systems**.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the IT Technician via the St Alban's Help Desk and will also inform the Online Safety coordinator or DSL.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I will alert the schools named child protection officer Mrs D Boardman / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to senior member of staff / designated Child Protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- Staff that have a teaching role only: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policy.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date

Full Name (printed)

Job title / Role

Consent from parents- Included in Reception and New starters information pack.
Return slips kept in main office.

St Alban's R.C. School



E-Safety

Publication of work & images

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: _____ **Class:** *Reception*

Pupil's Agreement

- ☐ I have read and I understand the school e-Safety Rules.
- ☐ I will use the computer, network, mobile phones, internet access and other new technologies in a responsible way at all times.
- ☐ I know that network and internet access may be monitored.

Signed: _____ **Date:** _____

Parent's Consent for Publication of Work and Photographs

I agree that my son/daughter's work may be published both electronically and / or in a paper format. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

I understand that the school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Signed: _____ **Date:** _____

Please print name: _____

Please complete, sign and return to school

St Alban's RC Primary School
Blackburn
PARENTAL PERMISSION FORM

In line with GDPR (General Data Protection Regulations), we need parent/carer's permission for children to take part in activities which are part of school life. Please circle and sign below if you are happy for your child to be involved in the following:

- ◆ Can we use your child's photographs in:-
 School books and on displays around school YES/NO
 In the newsletter which is published on the website and a copy is sent home with each child YES/NO
 On our School website YES/NO
 On Facebook YES/NO
 In the press including their publications and websites YES/NO
- ◆ Can we use your child's name in:-
 School books and on displays around school YES/NO
 In the newsletter which is published on the website and a copy is sent home with each child YES/NO
 On our School website YES/NO
 On Facebook YES/NO
 In the press including their publications and websites YES/NO
- ◆ Can we video your child for the use of:-
 Displays around school YES/NO
 On our School website YES/NO
 On Facebook YES/NO
- ◆ To travel in a teacher's/other responsible adult's car with appropriate insurance and booster seats when necessary YES/NO
- ◆ To take part in a walk in the local area or local woods if appropriately supervised by School Staff YES/NO
- ◆ Any other activity which may be reasonably requested at the Headteacher's discretion YES/NO

This permission is effective throughout the period my child is a pupil at St Alban's RC Primary School and for a short period after they leave.

Please note you can withdraw your consent at any point in time by contacting office@st-albans-blackburn.ash.uk

Child's Name

Signed

Date..... Parent/Carer

Consent from parents- Included in Reception and New starters information pack.
 Return slips kept in main office.

Online Safety Survey for Pupils

Whether you use the Internet for social networking, gaming or studying, being online is probably a really important part of your life. While the Internet presents lots of opportunities for you and your friends, there are many hidden dangers and new types of risk. Please help us to better understand how you use the Internet at home by filling in this survey. It is anonymous, so no one will know who filled it out. We will use the results to plan how best to support you and keep you safe online at home and at school.

- ▶ 1. Do you have access to the Internet at home?
yes ☐ no ☐
 - ▶ 2. If yes, on what sort of device(s) can you access the Internet?
laptop ☐ desktop ☐ tablet ☐ phone ☐ games console ☐
 - ▶ 3. If you have the Internet at home, where in the house do you access it?
shared family space ☐ shared bedroom ☐ own bedroom ☐ other ☐
 - ▶ 4. Estimate how much time you spend on the Internet each day.
less than one hour ☐ 1-2 hours ☐ 2-3 hours ☐ more than 3 hours ☐
 - ▶ 5. Are there privacy controls set up on the device you use at home?
yes ☐ no ☐
 - ▶ 6. Do you talk with adults at home about safe rules for Internet browsing?
frequently ☐ sometimes ☐ rarely ☐ never ☐
 - ▶ 7. What do you do online? (Tick all that apply.)
chat ☐ play games ☐ social networking ☐ studying ☐ other ☐ none ☐
 - ▶ 8. Which social networking sites do you have accounts with? (Tick all that apply.)
Instagram ☐ Facebook ☐ SnapChat ☐ Twitter ☐ Oovoo ☐
Tumblr ☐ Playstation Live ☐ WhatsApp ☐ YouTube ☐ Flickr ☐
Xbox Live ☐ Badoo ☐ TikTok ☐ other ☐ none ☐
-

Online safety Survey for Pupils

- ▶ 9. Do you have the same friends online and offline?
yes ☐ some overlap ☐ no ☐
- ▶ 10. Do you know what counts as personal information and that this shouldn't be posted or written about online?
yes ☐ no ☐
- ▶ 11. Have you ever felt uncomfortable with something you have seen online?
yes ☐ no ☐
- ▶ 12. Do you know what to do if something or someone made you feel uncomfortable online?
yes ☐ no ☐
- ▶ 13. Have you ever met up with anyone in the real world that you only knew online to begin with?
yes ☐ no ☐
- ▶ 14. Would you like to learn more about online safety in school?
yes ☐ no ☐
- ▶ 15. Is there anything related to online safety that you would specifically like to know more about?

- ▶ 16. Is there anything else you would like to tell us or you think we should know?

Online Safety Survey for Parents and Carers

Whether through social networking, gaming or studying, being online dominates the lives of many children and is an integral part of their daily existence. While the Internet presents a wealth of opportunities for young people, there are many hidden dangers and new types of risk. Please help us to better understand how our pupils are using the Internet at home by filling in this survey. We will use the results to plan how best to support you and your children.

- Please select the year group(s) your child(ren) is/are in.
☐ EYFS ☐ Y1 ☐ Y2 ☐ Y3 ☐ Y4 ☐ Y5 ☐ Y6
- Does/Do your child(ren) have access to the Internet at home?
☐ yes ☐ no
- If yes, on what sort of device(s) can they access the Internet?
☐ laptop ☐ desktop ☐ tablet
☐ phone ☐ games console
- If yes, where in the house does/do your child(ren) access the Internet?
☐ shared family space ☐ shared bedroom
☐ own bedroom ☐ other
- Estimate the number of hours your child(ren) spend on the Internet each day.
☐ less than one hour ☐ 1-2 hours
☐ 2-3 hours ☐ more than 3 hours
- Do you know how to check the privacy settings on the device(s) your child is using?
☐ yes ☐ no
- How frequently do you check the privacy settings?
☐ weekly ☐ monthly
☐ infrequently ☐ never
- Do you regularly discuss safe rules for Internet browsing with your child(ren)?
☐ yes ☐ no
- What does/do your child(ren) do online?
☐ chat ☐ play games ☐ social networking
☐ studying ☐ other ☐ no idea
- Which social networking sites does/do your child(ren) have an account with?
☐ Instagram ☐ Facebook ☐ Snapchat ☐ Twitter ☐ Gooxo
☐ Tumblr ☐ WhatsApp ☐ Youtube ☐ Xbox Live ☐ PlayStation Live
☐ Flickr ☐ Badoo ☐ TikTok ☐ no idea ☐ other ☐ none
- Does/Do your child(ren) have the same friends online and offline?
☐ yes ☐ some overlap
☐ no ☐ no idea

12. Do you know how to check who your child(ren) is/are friends with online?
☐ yes ☐ no
13. Has/have your child(ren) ever met up with anyone in the real world, that they had only known online?
☐ yes ☐ no
14. If your child was being bullied online, would you know how to stop it?
☐ yes ☐ no
15. Do you know how to monitor/block/report inappropriate activity online?
☐ yes ☐ no
16. Please name any authority, government agency or regulatory body that help to protect children online.

17. Is there anything, related to online safety, that you would specifically like to know more about?

18. Would you like to learn more about online safety?
☐ yes ☐ no
19. Which would be the best way for you to learn more about online safety?
☐ newsletter ☐ session in school ☐ via school website

What Parents & Carers Need to Know about GROUP CHATS

WHAT ARE THE RISKS?

- BULLYING** - Group chats can be a place where bullying happens. Children can be excluded, teased, or bullied in a group chat.
- EXCLUSION AND ISOLATION** - Children can be excluded from group chats, which can lead to feelings of isolation.
- INAPPROPRIATE CONTENT** - Group chats can contain inappropriate content, such as bullying, sexual content, or hate speech.
- SHARING GROUP CONTENT** - Children can share group chat content with others, which can lead to further bullying or harassment.
- UNKNOWN MEMBERS** - Children can be added to group chats by someone they don't know, which can be a risk.
- NOTIFICATIONS AND SOUND** - Group chat notifications can be loud and annoying, and can be a distraction.

Advice for Parents & Carers

- CONSIDER OTHERS' FEELINGS** - Think about how your child might feel if they are excluded or teased in a group chat.
- TEACH SUPPORT, NOT JUDGEMENT** - Encourage your child to support others in the group chat, rather than judging them.
- PRACTISE SAFE SHARING** - Teach your child to think before they share anything in a group chat.
- AVOID INVITING STRANGERS** - Encourage your child to only invite people they know to group chats.
- SILENCE NOTIFICATIONS** - Help your child to manage their group chat notifications so they don't become a distraction.

Meet Our Expert - Dr. Sarah-Jane Hill, Child Psychologist, discusses the risks of group chats and how to keep children safe.

National Online Safety #WakeUpWednesday

What Parents & Carers Need to Know about MINECRAFT

WHAT ARE THE RISKS?

- PUBLIC SERVERS** - Minecraft has public servers where children can interact with strangers.
- GAMING** - Minecraft is a game, and like all games, it can be addictive.
- ADDITIONAL PURCHASES** - Minecraft has in-game purchases for skins, tools, and other items.
- SCARY ELEMENTS** - Minecraft has some scary elements, such as monsters and zombies.

Advice for Parents & Carers

- RESEARCH CONTENT CREATORS** - Encourage your child to follow Minecraft content creators who are safe and appropriate.
- CHOOSE THE RIGHT MODE** - Help your child choose the right Minecraft mode for their age and interests.
- HOST A PRIVATE SERVER** - Consider hosting a private Minecraft server for your child and their friends.
- ENCOURAGE BREAKS** - Encourage your child to take breaks from gaming.
- TALK ABOUT STRANGERS** - Talk to your child about the risks of interacting with strangers online.

Meet Our Expert - Dr. Sarah-Jane Hill, Child Psychologist, discusses the risks of Minecraft and how to keep children safe.

National Online Safety #WakeUpWednesday

ONLINE CONTENT

10 tips to keep your children safe online

The internet has transformed the ability to access content. Many apps that children use are dependent on user-generated content which can encourage freedom of expression, imagination and creativity. However, due to the sheer volume of content online, it is not possible for platforms to regulate and moderate everything, which means that children are exposed to inappropriate images, videos or audio content. Through this guide, we've created this guide to provide parents and carers with some useful tips on keeping children safe online.

- 1. MONITOR VIEWING HABITS** - What your child has been moderating, inappropriate content can still slip through the net.
- 2. CHECK ONLINE CONTENT** - Understand what's being shared or what access is being given to the internet.
- 3. CHECK AGE-RATINGS** - Make sure things are old enough to use this app and in the recommended age limit.
- 4. CHANGE PRIVACY SETTINGS** - Make accounts private and set content filters and parental controls where possible.
- 5. SPEND TIME ON THE APP** - Get used to how apps work, what content is available and what your child likes to watch.
- 6. LET CHILDREN KNOW YOU'RE THERE** - Encourage them to tell you if they see anything inappropriate or if they're worried.
- 7. ENCOURAGE CRITICAL THINKING** - Talk about what people might post online and how some posts could cause distress.
- 8. LEARN HOW TO REPORT & BLOCK** - Adapt those apps that children know how to use, like reporting tools on social media apps.
- 9. KEEP AN OPEN DIALOGUE** - If a child is discussing something online, listen to their concerns, empathise and offer support.
- 10. SEEK FURTHER SUPPORT** - If a child has been affected by something, they've seen online, seek support from your school's safeguarding team.

Meet Our Expert - Dr. Sarah-Jane Hill, Child Psychologist, discusses the risks of online content and how to keep children safe.

National Online Safety #WakeUpWednesday

What Parents & Carers Need to Know about ARTIFICIAL INTELLIGENCE (AI) SOLUTIONS

WHAT ARE THE RISKS?

- ROOM FOR INACCURACY** - AI solutions can be inaccurate, leading to incorrect information or decisions.
- REINFORCING BIAS** - AI solutions can reinforce existing biases, leading to discrimination.
- IRRELEVANT INFORMATION** - AI solutions can provide irrelevant information, leading to confusion.
- LACK OF ACCOUNTABILITY** - AI solutions can lack accountability, making it difficult to identify who is responsible for errors.
- STYLING CREATIVITY** - AI solutions can limit creativity, as they often rely on pre-existing data.

Advice for Parents & Carers

- CREATE A SAFE ENVIRONMENT** - Encourage your child to use AI solutions in a safe and appropriate way.
- PROMOTE CRITICAL THINKING** - Encourage your child to think critically about the information provided by AI solutions.
- DISCUSS BIAS** - Talk to your child about the risks of bias in AI solutions.
- ENCOURAGE HUMAN INTERACTION** - Encourage your child to interact with people, rather than relying solely on AI solutions.
- CHECK SCHOOL RULES** - Check your school's rules regarding the use of AI solutions.

Meet Our Expert - Dr. Sarah-Jane Hill, Child Psychologist, discusses the risks of AI solutions and how to keep children safe.

National Online Safety #WakeUpWednesday

Examples of home- school communications with parents.