



St. Christopher Primary School

E-Safety Policy

1. Core Principle:

The most important aspect of keeping young people safe online is education. Children and young people need the help and support of our school to recognise and avoid e-safety risks and build their resilience, to ensure that they are not at risk when they are outside the safe environment provided by school. Age-related guidelines for the appropriate use of digital technology will be embedded throughout the curriculum and reinforced in dedicated assemblies, Computing and personal, social, health education (Jigsaw) lessons. We aim to teach pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, how to take responsibility for their own and others' safety and how to be responsible users of technology to reduce the likelihood of harm. Pupils will be supported to search and share safely and taught to evaluate the content that they access online.

Technology offers unimaginable opportunities and is constantly evolving. The Internet is now an essential element of education, business and social interaction. The school aims to provide students with quality Internet access and current technology to enrich and extend learning.

As technology is an integral part and fast-changing element of children's lives, it's essential that all staff work towards making such technology accessible but also that the access is managed appropriately. Many children enter school having had access to internet-enabled devices or having their own internet-enabled devices to use at home under supervision.

To this end, we all share a responsibility to ensure we create safe and responsible users who are aware of their own responsibilities as future digital citizens. Staff will receive training in how to embed e-safety throughout the curriculum, through PSHE lessons and through dedicated e-safety sessions. Sometimes these updates will happen pre-emptively based on emerging trends and the impact of this will be monitored and evaluated as necessary.

Children spend most of their time online or using these devices outside of the school environment so it's essential we develop relationships with parents to promote and, where necessary, educate the safe and appropriate use of these technologies.

2. Managing Internet Access

All pupils have internet access through their own Google Account. Pupils are taught how to use their Google Accounts safely and will regularly browse the internet and produce documents using their accounts on iPads and Chromebooks in school and on their own devices at home. Google Chrome is used as a safer internet browser. Pupils are encouraged to communicate using email within their Google Accounts.

All staff must read and sign the 'Acceptable ICT Use Agreement before using any school ICT resource.

School ICT systems' capacity and security will be reviewed regularly. Access is filtered using Smoothwall. Filtering will deny access to sites deemed not appropriate in school. Staff can encourage children to use specific search terms to reduce the likelihood of coming across unsuitable 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. Importantly, we aim to teach pupils to use their judgement in accessing websites and to learn to navigate away from inappropriate sites.

Virus protection will be updated regularly as part of the school's IT support provision.

Staff are informed of the appropriate use of ICT for work purposes, appropriate use for personal purposes and ways in which it will be regulated. They will be made aware of the sanctions issued if misuse is carried out.

3. Published content and the school web site

The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The head teacher has overall editorial responsibility to ensure that content is accurate and appropriate, however the responsibility to monitor the website can be delegated to the Website leader.

4. Publishing pupil's images

Parental permission will be sought for images of pupils to be published on the school website or in other school documentation. Parents should contact the school should they wish to withdraw permission.

Photographs that include pupils will be selected carefully.

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs in accordance with GDPR guidelines May 2018.

5. Social networking and personal publishing

The school will block/filter children's access to public social networking sites unless a specific use is approved.

Aspects of social networking will be taught to children (for example, email). Pupils are advised how to manage safe and responsible sharing of digital media online, using the appropriate privacy settings and permissions.

6. Managing filtering

The school will work with the LA, DfE 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 school office, who will report it to the LA to ensure that it is filtered out. Regular checks will be made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Impero extensions are used on Chromebooks to monitor for inappropriate language.

Impero is also used to monitor Windows based computers.

Regular reports are monitored by Senior Leadership.

If a pupil is deliberately attempting to access known inappropriate sites or is trying to circumvent the filtering system through use of VPNs, extensions, DNS hack, proxy websites or other technical methods, that user may have their access to Chromebooks and iPads in school suspended through their Google Account.

7. Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. They are free to use these devices in school but out of sight of children and outside teaching time. Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances and on school educational visits. Neither staff or visitors to school should take photographs of children on personal mobile phones or other personal devices.

Pupils are not currently permitted to bring their personal hand held devices into school but if children bring them into school as a safety precaution for walking home alone, for example, they need to be handed in to the school office. These devices will be turned off during school hours and while they are stored on-site.

8. Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Staff training will take place in light of changing technologies and procedures will be reviewed frequently in light of new technologies that emerge e.g. VR/AR, cloud computing etc. To this end, although systematic reviews and evaluation of the e-safety policy will be completed regularly, staff will be given the ability to question whether amendments or changes are needed as new technologies emerge and become prevalent based on their experiences in class or as new issues arise.

Wearable Technology: This is a developing technology and there is some crossover with existing technologies e.g. wristwatches. This will be subject to change as technology moves on and new features are added to consumer devices. The details below are a broad guideline and exceptions may have to be made as the proliferation of features to cheaper devices lowers the barrier to entry and more of these devices are marketed towards children e.g. Fitbit Ace.

Acceptable devices: At this point, basic 'fitness tracker' style bands are acceptable in school as long as their functionality is basic and the value of this device is comparable to a watch. In this case, the device will be worn at its user's risk.

Unacceptable devices: Any device which contains more advanced hardware and capabilities is not allowed in school. This includes devices which are capable of:

- running dedicated apps e.g. games
- have in-built data capabilities similar to a phone (e.g. 3G, 4G, 5G)
- have camera functionality
- have audio recording functionality

Examples of devices in this category would include Apple Watches, Fitbit Ionic/Versa/Blaze and similar models, Vtech Kidizoom and similar.

9. Protecting personal data

Personal data will be recorded, processed, transferred and made available in accordance with GDPR guidelines May 2018.

10. Handling E-Safety complaints

Complaints of Internet misuse incidents will be dealt with by a senior member of staff. Staff should report incidents/complaints to their line manager or the Senior Leadership Team.

Any complaint about staff misuse must be referred to the Head Teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Staff to report any concerns to their designated safeguarding lead. The school will keep a log of all incidents, including a description of the incident, details of who was involved and any actions taken. The log is kept online.

11. Extremism/Radicalisation

All staff and Governors will be familiar with the indicators of vulnerability to extremism and radicalisation and the procedures for dealing with concerns. Staff are made aware of the potential indicating factors when a child is vulnerable to being radicalised or exposed to extreme views. These include peer pressure, influence from other people or the internet, bullying, crime and anti-social behaviour, family tensions, race/hate crime, lack of self-esteem or identity, prejudicial (damaging) behaviour and personal or political grievances. Staff to report any concerns to their designated safeguarding lead.

11. 'Sexting'

All staff and Governors will be familiar with the process to respond to incidents involving 'sexting'. All incidents will be managed in line with the Safeguarding policy.

Written: September 2020

Approved by Governors:

Reviewed:

Appendix:

Twitter Usage Guidelines

Google Education Guidelines KS2

Google Education Guidelines KS1

Twitter Usage Guidelines

Aims of Using Twitter:

To share and celebrate children's achievements, successes and school updates.

To demonstrate safe and responsible use of social media.

To encourage the use of 21st Century technology

•The school Twitter account will be a Public account. Senior leaders will monitor the followers and block any who appear to not be school focused.

•The school Twitter account will only tweet between the hours of 8am and 6pm between Monday and Friday. The only tweets outside of this time are for school events (e.g. football matches, residential trips, performances) or to share urgent school news (e.g. closures due to adverse weather).

•The school Twitter account will only follow educationally linked accounts. No personal accounts, unless they are educationally linked (e.g. a children's author), will be followed.

•The school Twitter account will not reply to any 'replies' on Twitter. This is not the platform to discuss or debate school related issues. Senior Leaders may only reply if it is urgent (e.g. a question about a child while on a residential trip.)

•The school Twitter account will only use children's first names when referencing children.

•The school Twitter account will use Twitter to share positive messages about the school.

•The account may be used to share news and information during a school trip. The account will be run 4G/5G enabled phone for the period of the trip.

•Use of the @twittername of individuals is to be avoided (e.g. "excited about @dewnott speaking to us").

•By endorsing twitter we may be encouraging children to use twitter so reinforce e-safety rules such as "Never tweet anything that would be potentially upsetting; make sure you know how to report to anything you find that disturbs you; be careful who you talk to they may not be all they appear; never meet anyone from twitter world without telling your parents."



A Guide to G Suite for Education (Y3-6)

As part of our Computing Curriculum, the school is introducing a service called **G Suite for Education** (previously known as *Google Apps*). This new service is powered by Google and we will be joining over 8 million other pupils and teachers that are already using G Suite at schools around the world.

The service will give our children and staff access to a set of tools which will support the high levels of collaboration that are required in today's classroom to prepare students with communication and collaboration skills for life. G Suite will also enhance the delivery of not only our Computing curriculum, but lessons cross curricular.

In order to keep you informed and also to comply with data protection legislation and Google's Terms of Service, we are required to get parental permission (See <http://goo.gl/D9GNB6> for more information)

What's included in G Suite?

- **Gmail** provides email storage with extra security including restricted incoming and outgoing email access. **Emails by pupils are restricted to within St. Christopher's ONLY.** These email communications are monitored and recorded. *Pupils will NOT be able to send and receive emails outside of our school community* e.g. jbloggs@stchrisprimary.co.uk
- **Google Docs** is like Microsoft Word and lets pupils create and share written work, tables and forms. This also allows pupils to work collaboratively on projects simultaneously in real time. Several pupils will be able to work on the same document from their own homes.
- **Google Slides** is like Microsoft PowerPoint. It allows pupils to create presentations much more easily than in PowerPoint and easily add photos, videos and text from online sources or photos and videos they've taken themselves with just a couple of clicks. Pupils can also work collaboratively on a presentation if they choose.
- **Google Sites** makes it easy to collect, share, and publish all types of content in a single website. Children can create their own websites. Pupils will also be using sites to create portfolios of work.

What are the benefits of G Suite?

- **Ease of access:** Pupils can access G Suite at anytime, anywhere. It is designed to work in any browser (Google Chrome, IE, Firefox etc.) and on any computer or tablet or even phone This enables access to your documents and files (Word, Excel, PowerPoint and Publisher alternatives) from school or at home.
- **Unlimited Online storage:** No flash drives (memory sticks etc.) are required with documents and files stored online in Google Drive. Children can even create homework using G Suite and share with a teacher with one click.
- **Collaboration between students:** Children can work together on group projects, even in different classrooms. During collaborative work teachers can monitor progress of each child and provide instant written feedback visible to the group or to the individual. This enhances teaching and learning and provides instant and accurate assessment.

What about security and safety?

- There will be no advertisements.
- No external email addresses can contact pupil accounts and vice-versa.
- All email communication and comments within collaborative work are monitored. This information will be used in conjunction with the behaviour policy.
- Work uploaded to Google Drive remains the property of the creator; it is not copied or kept by Google if it is removed by the creator.
- Accounts are password protected and passwords can be reset if necessary by a member of staff.

How will G Suite be accessed?

Pupils will be shown how to use G Suite within the Computing Curriculum as part of the e-safety modules. Pupils will be provided with unique usernames and passwords. Parents/Carers are encouraged to explore G Suite with their children by logging in together and accessing their school work stored in G Suite. Pupils will follow school policies for appropriate use when using these tools. Pupils know that the school has the right and ability to monitor user accounts for policy and e-safety purposes as well as having the ability to remove access or suspend accounts if necessary.

Summary

G Suite is an essential part of the curriculum, for all subjects. Pupils without parental permission will be unable to participate in any lessons across the curriculum using G Suite. All email communication is archived and the school's Acceptable Use Policy will be enforced. School staff will monitor the use of G Suite when pupils are at school. Parents/Carers are responsible for monitoring their child's use of applications when accessing G Suite apps from home. Pupils are responsible for their own behaviour at all times.

We are excited to be bringing these tools to the school. If you have specific questions regarding how we use G Suite or for information on how it works please speak to Mr. Nagra.

How can I use this at home?

G Suite is best accessed via a laptop or desktop computer running a modern browser e.g. Chrome, Firefox. If you have an Android tablet or iPad we encourage you to visit the Play Store/App Store and install the following apps: **Google Slides, Google Docs, Gmail and Google Drive**. Google Drive is where all the files your child creates are stored and has unlimited cloud storage. You can export any file to Drive including large video files which can then be shared directly with teachers or other pupils if they are working collaboratively. Google Drive can also accept files from other apps. This can mean your child could create a presentation, written document, audio or video and then share these files instantly with a teacher as part of a homework task. This means no more lost USB sticks or emailing large files. For more information or help please check here:

<https://goo.gl/J9q55U>

<https://goo.gl/npa9Ry>

<https://goo.gl/a86N8X>

<https://goo.gl/Shslly7>

What happens next?

Your child will have an account created for them which they can use in school or at home. If they already have an account it will continue to function as normal.

If you do not wish your child to have access to these services please write to the school stating this.



KS2 Digital Technology Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should also have an entitlement to safe internet access at all times.

Children in KS2 will be provided access to Google Apps for Education, the details of which will be explained in a separate document.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour inside and outside of school

What will the school do?

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents and carers will be aware of the school expectations of the young people in it's care.

What do I need to do?

Parents are requested to read carefully the statement overleaf which outline the expectations of children in the school's care regarding their use of digital technology. You may wish to read through this with your child if you feel it's necessary. Details are also provided of the responsibilities and expectations of staff to ensure children can access and utilise these technologies safely.

As a parent/carer, I understand that:

- The school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- The school will take every reasonable precaution, including robust monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems.
- The school uses a firewall and filtering system to automatically block inappropriate content automatically.
- The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and websites.
- My child's activity on the systems will be monitored and recorded to ensure their safety and to prevent misuse. The school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- My child will be encouraged to treat digital devices with care and respect, handling them carefully and sharing them with others where necessary.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As a pupil of St Christopher Primary School, I understand that:

- When using the internet, I will think about the websites I'm accessing.
- If I find a website or image that is inappropriate, I turn off the monitor and I will tell my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site.
- I know that the Internet is provided for pupils to find information, practice skills and communicate with others. It is not for online gaming outside of lessons.
- Internet access is a privilege, not a right and that access requires responsibility.
- Unauthorised use of the Internet or use of unauthorised websites will not be tolerated.
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I will not look at other people's files or documents without their permission.
- I will not logon using another person's account (with or without their permission).
- I will think before deleting files.
- I know that the teachers can, and will, check the files and websites I have used and visited.
- I know that, when using G Suite (Google Apps), teachers can and will check the emails that I send and receive.
- I will take care when using the computers and other school equipment.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers but NOT other pupils.
- I will not install any software without permission from a teacher.
- I will not change the wallpapers or settings of iPads or laptops e.g. adding a passcode, changing the wallpaper to something inappropriate, try to install apps etc.

**I understand that if I am acting inappropriately or don't follow the rules my access to some or all ICT resources can be suspended.
I also will be dealt with in accordance with the school's Behaviour Policy.**



St Christopher
Community Primary School



EYFS/KS1 Digital Technology Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should also have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour inside and outside of school

What will the school do?

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents and carers will be aware of the school expectations of the young people in it's care.

What do I need to do?

Parents are requested to read carefully the statement overleaf which outline the expectations of children in the school's care regarding their use of digital technology. Details are also provided of the responsibilities and expectations of staff to ensure children can access and utilise these technologies safely.

As a parent/carer, I understand that:

- The school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. This understanding will develop as the children become older.
- The school will take every reasonable precaution, including robust monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems.
- The school has a filtering system which automatically filters out inappropriate content online.
- The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and websites.
- My child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- My child will be encouraged to treat digital devices with care and respect, handling them carefully and sharing them with others where necessary.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

