

Online Safety Policy

Contents

1. Introduction
2. Roles and Responsibilities
3. Acceptable use policies
4. Education of online safety
5. Technical – infrastructure/equipment, filtering and monitoring
6. Online presence- digital images, videos and social media
7. Online remote access learning
8. Responding to incidents of online misuse

1. Introduction

Executive Head teacher: Mark Ward

Head of school : Emily Alty

Designated Safeguarding Lead: Emily Alty

Deputy Designated Safeguarding Lead(s): Mark Ward

Link Governor for Safeguarding: Rachael Baker

Chair of Governors: Rachael Baker & Rob Joy (co-chairs)

Computing Lead: Rochelle Markwick

PHSE/RSE Lead: Emily Alty

Online safety Leads: Emily Alty / Rochelle Markwick

ICT technical services provider: APEX

Policy Date: October 2023

Policy Review Date: Annually, October 2024 (or more frequently if required, in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.)

This policy applies to all members of our St Thomas' community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of technology, both inside and outside of school. This policy cross-references information from St Thomas' Child Protection Policy and 'Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings', DFE 2019.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school/academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.



St Thomas' will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where Jesus said, 'Come follow me, live your lives the way God wants you to.'



known, inform parents/carers of incidents of inappropriate online safety behaviour that take place both in and out of school.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school/academy:

Governors/Board of Directors

Link Governor for Safeguarding is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of the Online Safety Governor/Director will include:

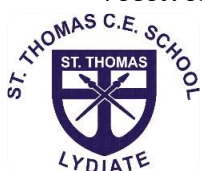
- regular meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering control logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority/MAT/other relevant body disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Leads

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT/relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (use of CPOMS).



Jesus said, 'Come follow me, live your lives the way God wants you to.'



- meets regularly with other safeguarding leads to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the school's/academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school/academy meets required online safety technical requirements and any Local Authority/MAT/other relevant body online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leaders/Online Safety Lead for further action to be taken
- that monitoring software/systems are implemented and updated as agreed in school/academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school/academy online safety policy and practices
- they have read, understood and signed the staff acceptable use policy. They report any suspected misuse or problem to the Headteacher/ Online Safety Lead/ for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and through discrete teaching
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead/Designated Person/Officer

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

Jesus said, 'Come follow me, live your lives the way God wants you to.'



- online-bullying

3. Acceptable use policies

Pupils are responsible for using the school digital technology systems in accordance with St Thomas' acceptable use agreements. Children agree to abide by the statements within the acceptable use policy. This is sent home annually to read with parents/guardians and sign. (See appendix A).

Remote Home Learning statements

- I will find a suitable learning environment to work in. I will need a table and chair within an enclosed space which is public but quiet, like a dining room. I agree not to work in my bedroom as this is my own private space.
- There will be an adult in the room whilst I am having my lesson. Even if I don't need their help, they will be there to make sure I am safe online.
- I will make sure that I am wearing appropriate clothing for my lesson, for example not my pyjamas. Anyone else who might be seen on my camera will also need to make sure they are dressed appropriately.
- I will ensure I still SLANT during remote learning, as I would in class. I agree not to be distracted by things like eating, playing with my pet, reading books etc.
- I will stick to deadlines, making sure I am on time for my lessons and that my Seesaw work is submitted for the time my teacher has asked for it and is of my best ability.
- During a lesson, I will keep my microphone on mute unless I am told otherwise by the teacher. I will not chat to others during the lesson or use the chat function unless we have been asked to do so by the teacher appropriately.
- I will use my real name for my lesson so that my teacher knows who I am. I will not add emojis or symbols to my screen-name.
- I will not take photographs, screenshots or record during the lesson. Filming or photographing others without their permission could get me in a lot of trouble.

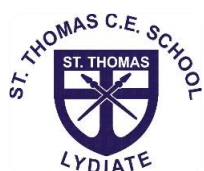
Parents/Guardians

St Thomas' recognise that parents and guardians play a crucial role in ensuring that their children understand the need to use technology in an appropriate way. St Thomas' will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school/academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line social media content (i.e Twitter)

4. Education of Online Safety

St Thomas' recognises the need for our pupils to take a responsible approach to staying safe online. The education of our pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. In planning our online safety curriculum, we have predominantly accessed information from the Government's 'Education for a Connected World -2020' document and 'HeartSmart' (PHSE curriculum).



Pupil Education

Jesus said, 'Come follow me, live your lives the way God wants you to.'



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

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and is regularly revisited (See St Thomas' Online Safety Knowledge Overview)
- Key online safety messages should be reinforced as part of a planned programme of assemblies and class activities (PHSE/Computing)
- Pupils are taught in all relevant lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information (PHSE/Computing)
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet (Computing)
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (PHSE/Computing)
- Evidence of Internet Safety to be documented in individual class PHSE scrapbooks.
- Pupils should be helped to understand the need for our St Thomas' acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Swiggle.co.uk has been set as the homepage on all in school desktop PCs, this is a child-friendly search engine, safe search results.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parent Education

We recognise that some parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of their child's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Newsletter bulletins
- School web site, with reference to relevant information, top tips and external websites
- High profile events/campaigns e.g. Safer Internet Day
- Information hand-outs e.g. Vodafone Digital Parenting Magazine



Jesus said, 'Come follow me, live your lives the way God wants you to.'



Staff/Governors

- All staff and governors receive annual safeguarding training, which encompasses online safety.
- Staff receive weekly safeguarding updates from a Designated Safeguarding Lead, these can be linked to online safety.
- Staff are aware of the relevant internet safety content to be taught in all year groups, and know that this may need to be adapted to suit the needs of their cohort. A whole school online safety curriculum is provided as part of Computing/PHSE/other lessons and is regularly revisited (See St Thomas' Internet Safety Knowledge Overview)
- The Online Safety lead (or other Safeguarding lead) will receive regular updates from external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and relevant accompanying documents will be available for all staff to access.

It is essential that all staff, including governors and visitors to the school understand their responsibilities, as outlined in this policy. Everyone is also made aware of the following information from 'Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings', DFE 2019. All adults agree that they will **NEVER**:

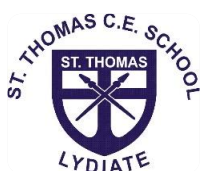
- Give personal contact details to pupils or communicate outside of school using social networks, email, text, twitter, etc. or meet a young person out of school unless part of a planned school activity with the knowledge of your Line Manager.
- Have conversations on social networking sites that make reference to children, parents or other colleagues at the school or be derogatory about the school. Never make any statements or post images on social networking sites that might cause someone to question your suitability to act as a role model to young people or bring your own or the school's reputation into disrepute.
- You should never communicate with parents through social network sites and you are strongly advised to declare any existing friendships/relationships to your Line Manager.
- Use personal equipment to photograph children (always use the school's equipment) and ensure any photographs are only stored on the designated secure place on the school's network and not on portable equipment.
- Should not post on the school's website or social media accounts any photographs of children without their consent. (Some children may be put at risk by their whereabouts being made publicly)
- Use your personal mobile phone (or other personal IT equipment) in areas used by children unless in emergencies or under an agreed protocol set out by the headteacher. In early years settings mobile phones should be locked away rather than carried by staff in areas occupied by children.

5. Technical – infrastructure/equipment, filtering and monitoring

Although our technical systems are managed by APEX, St Thomas' is responsible for ensuring that our network is as safe and secure as is reasonably possible. We maintain that policies and procedures approved within this policy are implemented, and that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

Technical systems will be managed in ways that ensure St Thomas' meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of school technical systems
 - Servers, wireless systems and cabling are securely located and physical access restricted



Jesus said, 'Come follow me, live your lives the way God wants you to.'



- All users will have clearly defined access rights to school technical systems and devices
- All users (within KS2) will be provided with a username and secure password and are reminded to be responsible for the security of their username and password.
- The administrator passwords for the school systems, used by the Network Manager (or other person) must be accessible to the Headteacher or other nominated senior leader
- School business manager and ICT technical services provider are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations, as we recognise that inadequate licencing could cause the school to breach the Copyright Act
- Internet access is filtered for all users. Appropriate content lists are regularly updated and there is a clear process in place to deal with requests for filtering changes (APEX folder).
- The school/academy has provided enhanced/differentiated user-level filtering (allowing staff more access i.e Google images/YouTube).
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.

The school has access to a range of technological equipment including desktop PCs and interactive screens in all classrooms, a laptop trolley, a set of iPads (kept in a trolley in the computing suite), and individual class iPads (1 per class). There are also desktop PCs in the 3 offices at the front of school and in the PPA room in the staffroom.

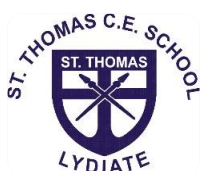
Mobile technology devices may be school owned/ personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud- based services such as email and data storage. All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies.

All staff have a password-protected, personal school email account, for school related emails. Parents wishing to contact staff by email will use the admin account and not the accounts of individuals.

6. Online presence- digital images, videos and social media

The development of digital imaging technologies has created significant benefits to learning. St Thomas' uses a Twitter account to share information and celebrate home-school learning. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. St Thomas' will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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



Jesus said, 'Come follow me, live your lives the way God wants you to.'



- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press (consent given when children start school)
- Parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Images taken by staff and volunteers must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, videos and their work.

With an increase in use of all types of social media for professional and personal purposes; we emphasise the following core messages regarding social media use, for the protection of individuals, the school and our MAT.

- No reference should be made in social media to pupils, parents/guardians or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /individuals
- Security settings on personal social media profiles should be checked and unable to be freely accessed by all
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to staff to upload content online (website and Twitter). These sites are password protected and staff agree to keep the information secure.
- The school should effectively respond to social media comments made by others according to a defined policy or process

7. Online remote access learning

In the rare occasion when children are not physically attending a school, St. Thomas' CE will consider the safety of our children when they are asked to work online. The starting point for online teaching remains the same as the principles set out in our school's staff code of conduct. Any online learning tools or systems recommended for use by St. Thomas' CE, will be in line with privacy and data protection/GDPR requirements. Staff will need to be mindful of what content is made publicly available online, and ensure that copyright is adhered to i.e. use of textbooks/copying reading materials.



Children, staff and parents will be issued with guidance and reminders about appropriate use of available platforms, whilst referring back to previous work in school around e-safety including appropriate

Jesus said, 'Come follow me, live your lives the way God wants you to.'



content and how to report inappropriate behaviour. guidance. Communication with parents will reinforce the importance of children being safe online. Families will be made aware of what their children are being asked to do online, including the sites they will be asked to access and who their child is going to be interacting with online, including members of staff from our school. Children are made aware of the agreements made in 'St Thomas' Acceptable Use Policy for Remote Home Learning'

Guidance to staff regarding 'live teaching', particularly in relation to live streaming of lessons:

- Consider if the system includes online chat feature, and if this can be moderated.
- Consider Privacy settings before posting, ensure settings are set to private and can only be accessed with a password.
- If live video and audio is being used, there should be careful consideration of the location being used and that appropriate dress code is maintained.
- Staff should ensure that they have a unique Zoom user ID, which is password protected. When this password is shared with parents, staff should reinforce the need for it to be kept secure and not shared.
- Staff are reminded to access the advanced settings of Zoom, to turn off screen sharing. screen sharing disabled, anyone can take control of the meeting and display their screen, this has been highlighted as a huge safeguarding risk.

8. Responding to incidents of online misuse

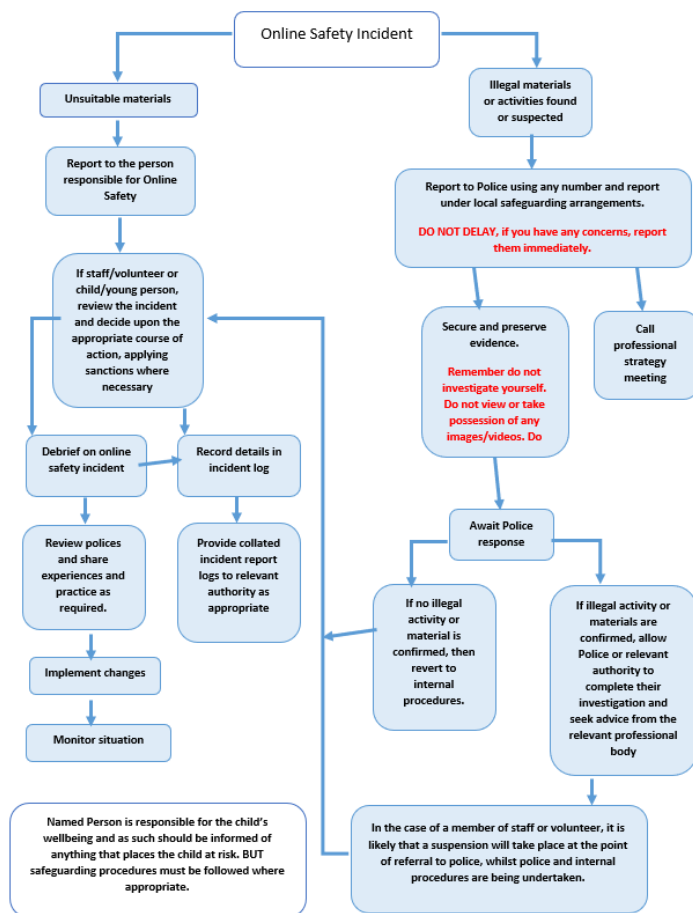
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities All incidents must be reported to a designated safeguarding lead as soon as they arise.

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



Jesus said, 'Come follow me, live your lives the way God wants you to.'





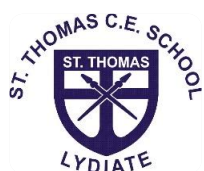
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child

- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

It is more likely that the school/academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.



Jesus said, 'Come follow me, live your lives the way God wants you to.'



Appendix A and B
Acceptable Use Policy for
EYFS & KS1
and KS2.



Jesus said, 'Come follow me, live your lives the way God wants you to.'



St Thomas' Acceptable Use Policy EYFS and KS1

A trusted adult is somebody who you know, they are people who care for you and want to make sure that you stay safe.



Examples of my trusted adults are:

_____ outside of school
and _____ at school.

Below are some statements to help make sure you stay safe and happy. Can you agree to them all?

		✓ if you agree
1.	I only USE devices or apps, sites or games if I am allowed to	
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 that online people aren't always who they say they are	
7.	I KNOW things I read online are not always true	
8.	Anything I do online can be shared and might stay online FOREVER	
9.	I don't keep SECRETS unless they are a present or nice surprise	
10.	I don't have to do DARES AND CHALLENGES even if someone tells me I must	
11.	I don't change CLOTHES or get undressed in front of a camera	
12.	I always check before SHARING my personal information	
13.	I always check before SHARING other people's stories and photos	
14.	I am KIND and polite to everyone	

Agreed and signed by _____ (child) Date: _____
_____ (parent/ guardian)



Jesus said, 'Come follow me, live your lives the way God wants you to.'



St Thomas' Acceptable Use Policy KS2



These statements can keep me and others safe & happy at school.

I learn online – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.

1. **I behave the same way on devices as face to face in the classroom, and so do my teachers** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
2. **I ask permission** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
3. **I am creative online** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
4. **I am a good friend online** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
5. **I am not a bully** – I know just calling something fun or banter doesn't stop it maybe hurting someone else. 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.
6. **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!
7. **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 app add-ons can cost money, so it is important I always check.
8. **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.
9. **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.
10. **If I make a mistake** – I don't try to hide it but ask for help.
11. **I communicate and collaborate online** – with people I already know and have met in real life or that a trusted adult knows about.
12. **I know 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.
13. **I never pretend to be someone else online** – it can be upsetting or even dangerous.
14. **I check with a parent/carer before I meet an online friend** the first time; I never go alone.
15. **I don't go live (videos anyone can see) 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.
16. **I don't take photos or videos or people without them knowing or agreeing to it** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
17. **I keep my body to myself online** – I never get changed or show what's under my clothes when using a device with 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.
18. **I say no online if I need to** – I don't have to do something just because someone 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.
19. **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.

Jesus said, 'Come follow me, live your lives the way God wants you to.'



20. **I follow age rules** – 13+ games, Apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
21. **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.
22. **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).
23. **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, at home and at school.
24. **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 and/or report it.
25. **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.
26. **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, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.

~~~~~

**I have read and understood this agreement.**

If I have any questions, I will speak to a trusted adult:

At school, that may mean: \_\_\_\_\_

Outside school, my trusted adults are: \_\_\_\_\_

I know I can also get in touch with [Childline](https://www.childline.gov.uk) (Tel: 0800 1111)

**Agreed and signed by** \_\_\_\_\_ (child)      **Date:** \_\_\_\_\_

\_\_\_\_\_ (parent/ guardian)



Jesus said, 'Come follow me, live your lives the way God wants you to.'

