Online Safety Policy

St Thomas the Martyr Primary School

Revised September 2021

Developing and Reviewing this Policy

This Online safety policy has been written as part of a consultation process involving the following people:

Mr C Roscoe

Miss M Deary

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

Policy created: November 2015

Revised: Annually. Sept 2021 (most recent)

This policy will be reviewed as appropriate by

Mr C Roscoe

Miss M Deary

Approved by C. Roscoe (Headteacher)

Approved by H. Foster (Governor)

Contents

Scope 3

Our schools vision for Online Safety 3

Roles and Responsibilities 3

Governors 3

Headteacher 3

Online Safety Champion 4

Teachers and Support Staff 4

Child Protection Officer 4

Online Safety Group 4

Pupils 5

Parents/Carers 5

Policies and practices 5

Education – students 5

Education – parents/carers 6

Education and Training – staff 6

Technical – equipment, filtering and monitoring 6

Use of mobile devices 7

Use of digital media 7

Data Protection 8

Communications – email 8

Communication - social media 9

Communication – school website 10

Communication – video conferencing 10

Acceptable Use Policy 10

Dealing with incidents 11

Standards and Inspection 12

Appendices – Acceptable Use Policies 12

Online Safety Policy

Scope

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to teaching and learning. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

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

Our schools vision for Online Safety
St Thomas the Martyr embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, St Thomas the Martyr aims to provide a safe and secure environment, which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Within the school the:

Computing coordinator: Miss M Deary

Online Safety Governor: Mrs S Osmond

Online Safety Champion: Miss M Deary

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Board of Governors has taken on the role of Online Safety Governor. The role of the Online Safety Governor includes:

- meetings with the Online Safety champion and Computing Co-ordinator
- monitoring of online safety incident logs

Headteacher

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 Champion.

- The Headteacher and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The Headteacher is responsible for ensuring that the Online Safety Champion and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Champion

- takes day to day responsibility for online safety issues
- 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 advice for staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering

Teachers and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current policies and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher and Online Safety Champion for investigation / action / sanction
- all digital communications with pupils / parents/carers should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety 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

Child Protection Officer

is 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
- online bullying

Online Safety Group

The Online Safety Group has responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group includes the Online Safety Champion, Computing Coordinator and the Online Safety Governor.

The group meets to discuss:

- the production / review / monitoring of the school online safety policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- including parents/carers in the teaching and learning of online safety

Pupils

- are responsible for using the schools digital technology systems in accordance with the Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school takes every opportunity to help parents understand these issues through assemblies, parents' evenings, newsletters, letters and the website etc.. Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- technology outside of school

Policies and practices

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety 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.

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

- A planned online safety curriculum is provided as part of Computing and PHSE lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and activities
- Pupils are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Planning will follow the objectives set out within the Education For a Connected World document published by the UK Council for Child Internet Safety.

Education – parents/carers

Many 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 / regulation of the children's on-line 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, therefore, seeks to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents/carers evenings / sessions
- Assemblies run by the children showing what they have learnt about online safety
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education and Training – staff

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

- A planned programme of formal online safety training are made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- This Online Safety policy and its updates are presented to and discussed by staff in staff meetings.
- The Online Safety Champion or Computing coordinator will provide advice / training to individuals as required.

Technical – equipment, filtering and monitoring

Our school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. Broadband connection, filtering and virus protection are provided (by default) by Virtue.

- School technical systems are managed in ways that ensure that the school 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 must be securely located and physical access restricted
- All users have clearly defined access rights to school technical systems and devices, e.g. username and password.
- All users are provided with a username and secure password. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager, is also available to the Headteacher and kept in a secure place.
- The school has legal ownership of all software.
- Mr J Purcell is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

- Only the administrator may download executable files and install software.
- Internet access is filtered for all users.
- The school encourages teachers to follow online safety policy guidelines when using laptop for personal use.
- If network monitoring takes place, it is in accordance with the Date Protection Act (1998).

Use of mobile devices

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

- All staff are aware that some mobile devices, e.g. mobile phones, games consoles or net books, can access unfiltered internet content.
- Devices are virus checked before use on school systems.
- Staff are aware that mobile phones are not to be used around pupils and must only be used in the staff room during the school day.
- It is against school rules for children to bring mobile phones, games consoles or any other valuable, desirable equipment onto the premises. If any of the above are taken into school for any reason, they must be kept securely locked away by the teacher until home time.

Please see Mobile Technologies policy for more information.

Use of digital media

Staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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

As photographs and videos of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), our school ensures that we have written permission for their use from the individuals and/or their parents or carers.

- 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, for example on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Parents/carers who have been invited to attend events are allowed to take photographs and videos but are made aware that they are for personal use only and must not be published on the internet or on any social networking site.
- 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.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All staff are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, once it has been transferred or its use is complete.

Communications – email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or

international. We recognise that pupils need to understand how to style an email and must have experiences of sending and receiving emails. The following statements reflect our practice in the use of email:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. The security of the password is the responsibility of the user.
- Users must immediately report to the Headteacher and Online Safety Champion the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Staff are provided with their own Lancashire lgfl email account to use for all school business.
- Any digital communication between staff and pupils or parents/carers (email, chat etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

Communication - social media

Many adults and pupils regularly use social network sites, e.g. Facebook, Twitter, Minecraft, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'locked' through the internet filtering system for direct use in school. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents are advised of the dangers that may arise from the use of social network spaces.
- Pupils will be advised to use nicknames and avatars when using communication sites.
- Staff and parents are aware that they should not publish pictures of other children on social networking sites. They are also made aware of the dangers of posting images of their own children.
- Pupils are taught about risks that may be associated with the use of social media, specifically in Years 5 and 6, in which they are taught about acceptable behavior when networking, keeping personal information safe and the importance of ensuring images are appropriate. Pupils in the years below are taught the foundations of these within a range of contexts.
- Children are taught about any new social media apps or websites that come to the attention of staff. The use of social media through gaming sites will also be addressed.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school 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* or local authority

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Any incidents of online bullying will are reported directly to the Headteacher. All incidents will be logged and regularly monitored. Parents will also be informed.
- Communication with parents or pupils does not take place on social networking sites.

Communication – school website

- Personal information staff or pupil personal contact information will not be published. The contact details given online will be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Permission from parents/carers will be obtained before photographs of pupils are published. Pupils' full names will not be used anywhere on the website or on newsletters particularly in association with photographs.
- Image file names will not refer to the pupil by name and will be stored securely on the network.
- The school website is linked to the school app. The above information also applies to the app.

Communication – video conferencing

- Permission from parents/carers will be obtained before children participate in video and photographs.
- Approval from the Headteacher must be obtained in advance of the video conferencing taking place. Pupils using video conferencing equipment will be supervised at all times.
- All staff supervising video conferencing equipment know the procedures to follow if they are unhappy with the content of a VC session, for example how to stop or hang up the call.

Due to systems put in place due to COVID, staff may now use video conferencing more regularly. Children can access lessons through Zoom and staff are informed of the expectations of these sessions. Staff may also communicate with the children and parents about school matters through the use of Microsoft Teams, if required due to school closure, bubble closure or children/staff isolating.

Acceptable Use Policy

Our Acceptable Use Policy (AUP) is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes (see appendix). The AUPs follow guidance from PurpleMash as this is our main software used.

AUPs are used for staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

Our school AUPs aim to:

- Be understood by each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the online safety policy/AUP.

- Outline acceptable and unacceptable behaviour when using technologies, for example: online bullying, inappropriate use of email, communication technologies, social network sites and any online content.
- Provide advice for users on how to report any failings in technical safeguards .
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of online safety education and its practical implementation.

The children will revisit the AUP's at the beginning of each school year and sign them. The AUP's are differentiated for children in EYFS, KS1 and KS2 (see appendix). The AUP's clearly state the expectations for children both in and out of the school grounds. They are discussed with the children and children sign to show that they will follow the AUP.

Dealing with incidents

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

At St Thomas the Martyr, an incident log is completes to record and monitor offences. This is audited on a regular basis by the Headteacher and Computing coordinator. It also forms part of the discussion with the Online Safety Governor during the Online Safety Group meeting that takes place termly. Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below, along with suggested sanctions:

Incident – accidental access to inappropriate materials.

Procedure and Sanctions:

- Minimise the webpage/ turn off the monitor.
- Tell a trusted adult.
- Enter the details in the Incident Log.
- Report to Sophos filtering services if necessary.
- Persistent 'accidental' offenders may need further disciplinary action.

Incident – using other people's logins and password maliciously, deliberately searching for inappropriate materials, bringing inappropriate electronic files from home.

Procedures and Sanctions:

- Inform Headteacher.
- Enter the details in the Incident Log.
- Additional awareness raising of online safety issues and the AUP with individual child / class.
- More serious or persistent offences may result in further disciplinary action in line with the Behaviour Policy.
- Consider parent/carer involvement

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
- 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.

St Thomas the Martyr may also take action against unacceptable use outside of school property. We do not tolerate actions that may affect staff/pupil wellbeing.

Standards and Inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.

At St Thomas the Martyr:

- Online safety incidents are monitored, recorded and reviewed.
- The Headteacher and Computing coordinator are responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is risk assessed.
- Incidents are analysed to see if there is a recurring pattern, for example: specific days, times, classes, groups and individual children.
- These patterns would be addressed most effectively through specific group work, class assemblies and reminders for parents.

Appendices – Acceptable Use Policies