Blackburn with Darwen L.A.

St. Thomas's Centre

Online Safety Policy

2025 - 2026

Introduction:

St Thomas's Centre recognises that Internet and Digital Technology are fantastic tools for learning and communication. Technologies are used in school to enhance the curriculum, and to challenge pupils through creativity and independence. Navigating through online content and digital media can present many positive opportunities, but it also leaves users exposed to security risks, abuse and harm. Online safety, is the knowledge of maximising the user's personal safety against security risks to private information and property associated with using the Internet, and self-protection from computer crime. It is important that all members of the school community are aware of online dangers and how they should conduct themselves online. Online safety is the responsibility of all pupils, staff and parents. There is a 'duty of care' for any persons working with children to educate all members of the school community on the risks and responsibilities of online safety. St Thomas's Centre is committed to conducting appropriate and good practice online.

Online safety covers the use of electronic communication devices: mobile phones, pcs, laptops, tablets, gaming consoles and how these devices can expose users to online harms, cyberbullying, sexual abuse, terrorist material, and illegal content. Technologies are used as tools to harm and exploit children. Cyberbullying is sending hurtful or abusive online media communication, texts and emails. Cyberbullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our Behaviour Policy. Online predators will entice users to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Users can be coerced into promoting terrorist material and forwarding illegal content.

It is important that there is a balance between controlling online access through technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating Digital Technology activity in school, and provide a good understanding of appropriate Digital Technology use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole- school issue and responsibility.

1. Roles and Responsibilities:

Governors
Governors are responsible for the approval of the Online Safety policy and for reviewing the effectiveness of the policy by reviewing online safety incidents and monitoring reports. Online safety falls within the remit of the Governor responsible for Safeguarding **Beverley Taylor**. The role of the Online Safety Governor will include:
- Ensure an Online Safety Policy is in place, reviewed annually and is available to all stakeholders.
- Ensure that there is an Online Safety Lead **Nicola Hulme** who has received appropriate training.
- Ensure that procedures for the safe use of online technology and the Internet are in place and adhered to.
- Hold the Headteacher and staff accountable for online safety

Headteacher and SLT
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. Any complaint about staff misuse must be referred to the Online Safety Lead at the school or, in the case of a serious complaint, to the Headteacher.
- Ensure access to induction and training in online safety practices for all users. Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable. St Thomas's

Centre monitor these on a weekly basis.

- Ensure that staff or external providers who operate monitoring procedures are supervised by a named member of SLT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect pupils are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership team will receive monitoring reports from the Online Safety lead.

Online Safety Lead

- Leads online safety meetings.
- Work in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect pupils are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports to Senior Leadership Team.
- Liaise with the nominated member of the Management Committee & Headteacher to provide termly reports on the number of online safety incidents reported and any action taken.

IT Technical Staff

- The IT Technical staff is responsible for ensuring:
- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any 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 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; Online Safety Lead for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

2.   Communicating School Policy

This policy is shared with all staff and governors on an annual basis and is also available from St Thomas's Centre school **O Drive-Policies** and website for parents, staff, and pupils to access. Rules relating to the school code of conduct when online and online safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used and during PSHE/SMSC where personal safety, responsibility and/or development are being discussed. The Online Safety policy is also re-issued to staff on an annual basis and after the policy review.

3.   Reporting Online Safety Incidents:

Online Safety Incidents should be reported in line with the school's policy on reporting safeguarding

issue (see Safeguarding Policy), i.e. face to face or via phone to Safeguarding Lead or Deputy Safeguarding Lead and/or on Synergy. This means appropriate action c an be taken in a timely manner, e.g. referrals to CADS, blocking websites, banning use of technology in school for individuals, etc.

4. Faulty ICT Equipment

If there is a fault with any equipment please report this immediately to the School Data & Exams Manager, Matt Grady by raising the issue on the school Every system.

5. Making use of ICT and the Internet in school

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the Internet in schools are:

For pupils:
- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Freedom to explore the world and its cultures from within a classroom.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self- evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.
- Access to remote online learning when isolating from school

For staff:
- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Class management, attendance records, schedule, and assignment tracking.
- Ability to provide immediate feedback to Pupils and parents.
- Ability to provide remote online learning when directed

For parents:
- Access to all school communication e.g. letters home, holiday dates etc.
- Access to resources to help Digital Parenting and a range of school policies.
- Information regarding school closure when weather is inclement.
- Curriculum information.
- Contact information.

6. Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet

content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Pupils who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the Online Safety Lead who will have the site blocked. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

7.   Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from SLT.

For more information on data protection in school please refer to our **Data Protection Policy available on the O Drive or school website**. More information on protecting personal data can be found in **section 11** of this policy.

8.   Emails

The school uses email internally for staff and pupils, externally for contacting parents and is an essential part of school communication. It is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, Pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right and will monitor emails and their contents if there is a valid reason of concern.

8.1 School Email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must follow GDPR guidance and refer to pupils using their initial only.
- Attached documents containing data or information about pupils should be encrypted or password protected.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Pupils should be aware of the following when using email in school:

Pupils will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:
- In school, pupils should only use school-approved email accounts
- Social emailing is restricted
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Pupils must not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated through the Online Safety Curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

9.   Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, Pupils and staff for keeping up-to-date with school news and events, celebrating whole-school achievements or personal achievements and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published and details for contacting the school will be for the school office only.

9.1   Policy and Guidance of Safe Use of Children's Photographs and Work

Colour photographs and pupils work bring our school to life, showcase our pupil's talents and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school, parents/carers will be asked to sign a

photography consent form. The school carries this out so as to prevent repeatedly asking parents for consent over the school year. The terms of use of photographs never change and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used.
- How long parents are consenting the use of the images for.
- School policy on the storage and deletion of photographs.

Using photographs of individual children

It is important that published images do not identify Pupils or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- No images at all should be taken, distributed or published for any reason of (Children In Our Care)
- Parental consent must be obtained. Consent will cover the use of images in:
    - all school publications
    - on the school website
    - in newspapers as allowed by the school
    - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a Pupil in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the Pupils such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school's **Safeguarding Children and Child Protection Policy**.

9.2   Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **Complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools **Child Protection and Safeguarding** policy and **Behaviour policy. All policies can be located on the school's website.**

Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. There are restrictions on the use of these sites in school that apply to both pupils and staff.

With regards to social media sites both pupils and staff should be aware of how they present themselves online. Pupils are taught through the Online Safety Curriculum, PSHE/SMSC, guest speakers and Safer Internet Day about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's rules regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction. Staff also receive regular online safety newsletters, updates and access to further guidance via emails, staff training and the school website.
- Staff should not give their personal contact details to pupils for example, e-mail address, home or mobile telephone numbers, details of web-based identities. If pupils locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their line manager. The child should be firmly and politely informed that this is not acceptable. ***Source: Guidance for safer working practice for those working with children and young people in education settings – 2022.***

10. Mobile Phones and Personal Device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying
- Can be used to access inappropriate material online
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

St Thomas's Centre requests Pupils switch off their mobile phone and hand in to staff until the end of the school day.

- The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the school's **Behaviour Policy**.

- A member of staff can confiscate mobile phones and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

10.1 Mobile Phone or Personal Device Misuse

Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff.

11. Cyberbullying

The school, as with any other form of bullying, takes Cyberbullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **Behaviour Policy.** The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:
- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

Repeated bullying may result in a fixed term exclusion.

12. Online Sexual Abuse

If a pupil discloses online sexual abuse, it will raise serious safeguarding issues should be reported using the normal child protection procedures. If in doubt please speak with the Online Safety Lead or a Designated Safeguarding lead.

If an allegation of online sexual abuse does come up, the school will:
- Take it seriously
- Act as quickly as possible to establish the facts.
- Record and report the incident
- Provide support and reassurance to the victim

If a pupil discloses a posting of a sexual image, the school will:
- Take it seriously
- Act as quickly as possible to establish the facts.
- Record and report the incident in accordance with Safeguarding procedures.

13. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

14. Access to remote learning

When using Remote Learning - Pupils
- Lessons must be conducted in communal areas such as kitchen/living room, not bedrooms.
- A parent or carer should be present in the communal area when lesson takes place.
- Pupils must "check in" and must be viewed by the teacher each lesson.
- Pupils must be appropriately dressed.
- Pupils must use appropriate language or behaviour as expected in the classroom.
- Pupils must make sure microphones are on mute unless being asked to contribute to the lesson
- Pupils must only use the chat facility when instructed to do so by your teacher

When using Remote Learning – Staff
- Lessons must be conducted in communal areas with a professional back screen
- Two members of staff to be present with a remote learning
- Staff must be appropriately dressed
- Staff must deliver lessons in a professional manner as expected in the classroom
- Staff must ensure the use of the chat facility is used appropriately by pupils
- If you are the lead presenter, you are responsible to always end meeting for all participants
- Report to your line manger if there are any concerns.

Parents/Carers responsibility for Remote Learning
- Enable remote lessons in communal areas which ensure my child can study.
- Ensure child appropriately dressed
- Be in the vicinity when a lesson is being conducted and monitor child's behaviour.
- Report to school if there are any concerns

15. Protecting Personal Data

St Thomas's Centre believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and Pupils.

In line with the Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) the school will use data:

- fairly, lawfully and transparently
- for specified, explicit purposes
- in a way that is adequate, relevant and limited to only what is necessary
- accurately and where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There may be circumstances where the school is required either by law or in the best interests of our Pupils or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguarding relating to data protection read the school's

Data Protection Policy on the school website**.**

Reporting activity

Report any concerns around radicalisation to a safeguarding lead, or by ringing the police non-emergency number 101 and / or the anti-terrorist hotline 0800 789 321.

Material that promotes terrorism or extremism can be flagged at www.gov.uk/report-terror

IF IN DOUBT ABOUT ANYTHING RELATING TO THIS POLICY REPORT TO THE SAFEGUARDING TEAM!!!