Saint Thomas More Catholic Primary School

Online Safety Policy

Consulted with staff	March 2023
Agreed by governor committee	March 2023
Ratified by full governing body	
Date for review	September 2024
Signature of Chair of Governors	
Signature of Headteacher	

1. **Intent**

Jesus Christ said 'Let the children come to me, do not hinder them' (Matthew 19:14). As a Catholic school it is our mission to educate pupils in such a way that no matter what their abilities or background they may reach their full potential as human beings. We thus seek to overcome any hindrance that might prevent any pupil accessing the fullness of the curriculum, opportunities and activities we offer.

2. **Safeguarding Statement**

'Saint Thomas More Catholic Primary School is committed to safeguarding and promoting the safety and welfare of all children and expects all staff and volunteers to share this commitment.'

3. **Context**

These procedures detail St Thomas More Catholic Primary School's whole school approach to online safety. At St Thomas More there is a whole school approach to online safety that goes beyond teaching to include all aspects of school life including culture, ethos, environment and partnership with all stakeholders within the school community.

This policy has been written with regard to the information and guidance as laid out in:

- Keeping Children Safe In Education 2022
- Teaching Online Safety in School
- Education for a Connected World – 2020 Edition
- Online Safety in Schools and Colleges: Questions from the Governing Board
- Vulnerable Children in a Digital World

The procedures work within and alongside the following policies:

- Child Protection and Safeguarding Policy
- Allegations Against Pupils Policy
- Allegations Against Staff Policy
- RSHE Policy
- CES Whistleblowing Policy
- Behaviour Management Policy
- Teacher Standards

Holy Cross Catholic MAC policies:

- HCC MAC Staff Code of Conduct
- HCC MAC Data Protection Policy
- HCC MAC Information Security Policy
- HCC MAC Anti-Bullying Policy
- HCC MAC Prevent Policy
- HCC MAC Remote Education Policy

- HCC MAC RSE Policy
- HCC MAC ICT and Internet Acceptable Use Policy

Within the Online Safety Policy fall the following:

- IT Alert Procedures
- Mobile Devices (including Phones) Policy

4. Roles and Responsibilities

4.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor the effectiveness of online safety through scrutiny of monitoring provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the Holy Cross Catholic MAC Acceptable Use of ICT and the Internet Policy
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).

4.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputy DSLs are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Computing Lead, Office Manager, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy

- Ensuring that any online safety incidents are logged using CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying or other online safety incidents are logged and dealt with appropriately in line with the Behaviour Management Policy, the HCC MAC Anti-Bullying Policy and the Child Protection and Safeguarding Policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Governing Board

This list is not intended to be exhaustive.

4.4 The MAC ICT, Communication & Compliance Manager (ITCC)

The ITCC manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any system-based online safety incidents are reported to the DSL so that they can be logged and are dealt with appropriately in line with this policy
- Ensure that filtering and monitoring alerts are working and sending.

4.5 Computing Lead

The Computing Lead is responsible for:

- The effective design of a clear progression of specific online safety learning within the Computing curriculum
- Monitoring the implementation of the curriculum to ensure full coverage
- Monitoring the impact of the online safety curriculum in enabling pupils to develop an understanding of online risks and ways of managing online safety effectively.

4.5 PSHE Lead

The PSHE Lead is responsible for:

- The effective design of the PSHE curriculum, including the RSE curriculum, to provide a spiral curriculum that has effective progression of learning in promoting knowledge and understanding of and the development of effective personal, social and health skills to equip pupils to be safe online.

- Monitoring the implementation of the curriculum to ensure full coverage
- Monitoring the impact of the PSHE curriculum in enabling pupils to develop an understanding of online risks and ways of managing online safety effectively.

4.6 RE Lead

The RE Lead is responsible for:

- Collaborating with the PSHE Lead to ensure an effective and age-appropriate RSE curriculum that equips pupils with the skills and understanding to manage all relationships, including those that occur wholly or partly online, in a positive and safe way.
- Collaborating with the PSHE Lead to monitor the implementation of the RSE curriculum to ensure full coverage
- Collaborating with the PSHE to monitor the impact of the RSE curriculum in enabling pupils to manage all relationships, including those that occur wholly or partly online, in a positive and safe way.

4.7 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the HCC MAC Acceptable ICT and Internet Use Policy and ensuring that pupils follow the HCC MAC Acceptable ICT and Internet Use Policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and the Child Protection and Safeguarding Policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’
- Responding appropriately to all reports and concerns about child-on-child abuse, both online and offline and maintaining an attitude of ‘it could happen here’

4.7 Parents

Parents are expected to:

- Notify a member of staff (usually your child’s class teacher in the first instance) of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

Keeping Children Safe Online (NSPCC)

UK Safer Internet Centre

Think U Know (CEOP)

Internet Matters

National Online Safety

4.8 Pupils

Pupils are expected to:

- Engage fully in learning that gives them the knowledge and skills to keep themselves safe online.
- Follow online safety rules in school and outside of school.
- Use devices and the internet in a positive way to safely enhance their learning.
- Never share their own or others personal or identifying information, including passwords, online.
- Never use the internet to behave in a way that is unkind or wrong. This includes cyber bullying, posting or viewing of inappropriate images, sharing inappropriate or offensive views or material and any other action which could cause offense, upset or be perceived as bullying.
- Report anything that makes them feel unsafe or uncomfortable to a member of staff or parent/carer (or trusted adult) immediately.
- Always work within the Acceptable Use of ICT and Internet Policy (Primary School Pupil version, Appendix 2)
- Not bring personal devices to school unless by express permission of a senior member of staff. (Year 6 pupils may bring mobile phones to school if they have a Walking Home Pass and walk to/from school unsupervised. All pupil mobile phones must be switched off when onsite and handed in to the office for the duration of the school day. The school does not accept responsibility for any mobile phones or other devices brought on to the school site.)
- Alert a member of staff immediately if they are aware of anyone using the internet in an unsafe or inappropriate manner.

Through the curriculum

At St Thomas More, online safety is taught explicitly through different areas of the curriculum as well as being reinforced in special days or events and through the ethos and culture of the school in the way the Behaviour Management Policy, Child Protection and Safeguarding Policy and in day-to-day lessons when technology is being used to enhance learning.

Pupils are taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and how to recognise and display respectful behaviour online. Pupils are taught how to stay safe online and how to behave appropriately online.

Online safety is taught in the following curriculum areas:

- **Computing** This includes how to evaluate what children see online, appropriate online behaviour and identifying online risks. Online safety is primarily taught through the Computing curriculum
- **RSE** This includes developing a strong sense of self, self worth and managing relationships safely and positively. This consolidates and supports the teaching of online safety within the computing curriculum.
- **PSHE** This complements and enhances the learning in RSE and also includes health, wellbeing and lifestyle behaviours. This consolidates and supports the teaching of online safety within the computing curriculum.

Beyond the curriculum, including through school culture

In addition, opportunities to complement and develop learning from within the curriculum are maximised. This includes maximising opportunities in other areas of the curriculum, for example when learning about persuasive writing in English; observing national events, such as Safer Internet Day and Anti-Bullying Week; responding to current affairs; responding to incidents as they occur and through the development of a respectful, tolerant and Christ-like culture within our school, where we *Learn and Grow as God's Holy People* through the focus of pupils and staff on the Jesuit Values and Virtues:

- Compassionate and loving
- Eloquent and truthful
- Learned and wise
- Curious and active
- Faith-filled and hopeful
- Intentional and prophetic
- Attentive and discerning
- Grateful and generous

Underpinning knowledge and behaviours

The online safety curriculum, taught through the computing curriculum, the RSE curriculum and the PHSE curriculum, covers the principles of online safety in EYFS, KS1 and KS2. Learning is designed with progression of content to reflect the different and escalating risks that pupils face as they mature and are exposed to different online risks. Learning is revisited and throughout the Key Stages to consolidate understanding and develop a greater depth of knowledge and develop pupils' ability to manage their own online safety with the support of trusted adults.

The online world changes and develops at great speed. Therefore it is important to focus on the underpinning knowledge and behaviours that can help pupils safely navigate the online world. Teaching will always be age and developmentally appropriate.

The document Education for a Connected World – 2020 Edition provides a clear guide of age appropriate learning that is divided into 8 areas. The online safety learning that takes place at St Thomas More has been cross-referenced against this learning to ensure that pupils receive a full online safety education at a level that is appropriate to them. For further information about the design of the online safety curriculum at St Thomas More, please see the Online Safety Skills and Progression document.

Underpinning knowledge and behaviours taught include:

- **How to evaluate what they see online** Enabling pupils to make judgments about what they see online and not automatically assume that what they see is true, valid or acceptable.
- **How to recognise techniques used for persuasion** Enabling pupils to recognise the techniques that are often used to persuade or manipulate others.
- **Online behaviour** Enabling pupils to understand what acceptable and unacceptable online behaviour look like: the same standard of behaviour, respect and honesty apply on and offline.
- **How to identify online risks** Enabling pupils to assess a situation, think through the consequences of acting in different ways and decide on the best course of action.
- **How and when to seek support** Enabling pupils to understand safe ways to seek support if they are concerned or upset by something they have seen online.

Online harms and risks

St Thomas More Catholic Primary School recognises that online risks can be described by 'the 4 Cs':

- **Content** Children may be exposed to inappropriate or harmful content online.
- **Contact** Children may be subject to harm from those they come into contact with online. This can include people with intent to groom, exploit or radicalise.
- **Conduct** Children may themselves behave in a way that is inappropriate or harmful to themselves or others online, for example sending or receiving explicit images.
- **Commerce** Children may be at risk of being taken advantage of through financial scams (cyberscams), online gambling, phishing or scams.

Meeting the needs of all pupils and recognising vulnerable pupils

St Thomas More Catholic Primary School recognises that any pupil can be vulnerable online, however there are some pupils who may be more susceptible to online harm. The research detailed in the Vulnerable Children in a Digital World Report highlights the risk of different groups of vulnerable children:

- **Children with a family vulnerability**, e.g. young carers or Looked After Children.
- **Children with communication difficulties**, e.g. those with English as an Additional Language (EAL), with speech and language difficulties or those who have hearing difficulties
- **Children with physical disabilities**, e.g. those with a physical disability, with vision impairment or with long-standing illness
- **Children with Special Educational Needs (SEN)**, e.g. those with learning difficulties or other SEN
- **Children with mental health difficulties**

The table below shows how children with different vulnerabilities may be at greater risk of different online harms.

Vulnerability	**Greater risk posed**	**Context** (data taken from 10-16 year olds)
Family vulnerability	• High risk of overall online harm in all areas • Particularly at risk of Cyberscams (**commerce**) • Being at risk of cyberscams often indicates further risk of online aggression • Being the victim of cyberscams can be predicted by those who have experienced exposure to inappropriate **content** and have been at risk of inappropriate **conduct**	• Looked After Children are 3 times more likely than their peers to try to get around blocks or filters; • 7 times more likely to have their personal details hacked; • 45% use chatrooms • 58% of Young Carers & 48% of those in care said they had been cyberbullied (compared to 25% of peers with no vulnerability) • Only 59% of young carers receive advice at home on online safety; only 31% of those in care receive online safety advice at home • More than half of young carers report spending more than 5 hours online a day
Special Educational Needs	• High risk of overall online harm in all areas • Particularly vulnerable to **contact** risks, e.g. sexting under pressure, coercion, blackmail. May not recognise	• One third more likely to say they were not taught how to stay safe online • One third more likely to say online safety education was 'useless'

	when they are being manipulated - Experiencing **contact** risks is associated with greater risk of **content** exposure, **conduct** risks and cyber aggression	- Significantly more likely to say they never follow online safety advice - Twice as likely to say online safety was given too early - Those with learning difficulties were one third more likely to spend more than 5 hours a day online and on third more likely to have their social media account hacked - 27% view sites promoting self harm (compared to 17% of non-vulnerable peers) - 25% view pro anorexia sites (compared to 17% of peers)
Communication difficulties	- Significantly vulnerable to all high risk scenarios - Significantly susceptible to cyberscams (**commerce**) and **conduct** risks - Significantly associated with experience of cyber aggression	- Young people with communication difficulties are more likely to visit gambling sites and spend more time in chatrooms - Young people with reading difficulties may struggle to understand details on websites and apps and so can be more susceptible to cyberscams (commerce) - Young people with hearing loss more likely (than peers) to be involved in sexting - Young people with hearing loss 5 times more likely to say 'the internet left me with thoughts and feelings that were upsetting.' - Young people with hearing loss twice as likely to be cyber bullied than non-vulnerable peers
Mental health difficulties	- Significantly high risk for all high risk online scenarios, rather than a single type of risk - Experiencing cyber aggression predicts the likelihood of	- 40% report having been cyber bullied (23% for non-vulnerable peers) - Gorzig (2016) found that both those who were cyberbullied and the perpertrators were

	experiencing all high risk online scenarios	more likely to view pro-suicide websites • More likely to post photos and share activities • More likely to visit sites displaying adult content
Physical disabilities	• Significantly more likely to experience all high-risk online scenarios • Particular risk for **conduct** risks	• Over half report spending more than 5 hours a day online • Parents/carers least likely to limit screen time. • 54% said parents/carers had taught them how to stay safe online • 32% said online safety education (from parents or schools) was not good enough or useless (compared to 8% of non-vulnerable peers) • More likely to visit sites with adult content • More than one third have social media hacked

- Boys are more likely to be involved in conduct risks; visit gambling sites or be tricked into buying fake goods.
- Girls network more actively and are impacted more severely by online misogyny and cruelty from anonymous disinhibited users.
- Young people who prefer not to state their gender are particularly at risk online.

Staff will be particularly vigilant in monitoring the online safety of pupils who may be additionally vulnerable and will seek to tailor online safety learning to the needs and vulnerabilities of individual pupils as appropriate. This may include:

- Targeting teaching and assessment of the different aspects of online safety to children within vulnerable groups
- considering whether especially vulnerable children have missed online safety due to absence and providing opportunities to ‘catch up’. This is one reason why it is important that online safety is embedded throughout the curriculum, and not just taught in discrete lessons.
- Considering the most effective way of sharing important online safety information: ‘scare stories’ have little impact in changing behaviour; having strong influences from people children are emotionally connected can be more effective

Research shows that once children have been identified as experiencing online harm, they are more likely to be found to be susceptible to other kinds of harm on or off line. Staff will be vigilant in considering contextual safeguarding - establishing an understanding of the whole child - in responding to incidents and vigilant in promoting the safeguarding of the child in all aspects of their life.

The DSL, Deputy DSLs and SENDCo will monitor those children who have been identified as at risk online during their half termly safeguarding monitoring.

Engaging parents and carers in online safety

St Thomas More Catholic Primary School has a whole school approach to online safety which includes engagement of parents and carers in promoting their child's online safety. We do this by:

- Sharing online safety resources and information with parents and signposting to recognised sources of information. This may be via direct emails, shared on weekly newsletters or in another way.
- Signposting parents to available courses designed to support parents and carers in promoting online safety for their child.
- Informing parents and carers if their child has been involved in an online safety incident and offering advice as appropriate.
- Inviting parents to online safety meetings as appropriate, e.g. in response to an identified online safety concern.

The views of parents and carers have been sought in the development of this policy.

Systems to promote online safety

The IT system used in school has firewalls and protection built in which safeguards school devices. These include Smoothwall, which is managed by Coventry City Council and Impero which is managed by the school. However it is important that all users remember that no IT system can be 100% effective and so staff and children must be confident in reporting online safety concerns.

The school uses Impero to monitor usage of any school device. This triggers an alert which enables the Headteacher (DSL) and Deputy Headteacher (DDSL) to monitor staff and pupil use and identify any inappropriate use when school devices are on or off site. To support this system, staff record the name of the pupil(s) using a device against the identification number of the device being used. The procedure followed when an alert is received is detailed in Appendix 1.

The DSL, DDSLs and the SENDCo meet half termly to review and monitor analysis of safeguarding information. This enables individual children representing an online safety concern to be identified and monitored and for trends to be identified and addressed.

Searching and screening of devices

Inline with the school's Mobile Devices Policy and DfE Searching, Screening and Confiscation, 2022, the Headteacher or Deputy Headteacher may search a child's belongings if there are reasonable grounds for suspecting that the pupil is in possession of a prohibited item or any item identified in the school rules for which a search can be made, or if the pupil has agreed. Staff will always refer and adhere to the Searching, Screening and Confiscation, 2022 guidance prior to carrying out a search. **No member of staff will ask to view an indecent or inappropriate image on a device.** Any device allegedly containing images retained as part of allegations of sharing of consensual or non-consensual nude images or videos (sometimes known as 'sexting') will be dealt with promptly and sensitively. Parents will be informed and a referral will be made to MASH/the police involving any child under the age of 13.

Parents should always be informed of any search for a prohibited item listed that has taken place, and the outcome of the search as soon as is practicable. A member of staff should inform the parents of what, if anything, has been confiscated and the resulting action the school has taken, including any sanctions applied.

If a pupil breaches school policy on online safety or the Mobile Devices Policy then the phone or device may be confiscated by a member of SLT, in-line with the Child Protection and Safeguarding Policy, Keeping Children Safe in Education and Searching, Screening and Confiscation, 2022,. Any action taken by a member of staff will prioritise safeguarding of pupils and will not contravene any school safeguardinga procedure. Any device that is confiscated will be held in a secure place in the school office. Mobile phones and devices will only be released to parents or carers after a conversation between the parent/carer and a member of SLT.

Breaches of online safety practice

All breaches of online safety will be addressed first and foremost as a safeguarding concern. Once safeguarding requirements have been addressed, other elements such as behaviour management will be addressed.

Breaches by staff

Any breach of online safety practice by staff will be addressed through the application of the appropriate policy: Child Protection and Safeguarding Policy, Staff Code of Conduct, Whistleblowing Policy, Low Level Concerns Policy and Disciplinary Policy (not an exhaustive list).

Any breach of online safety practice will be recorded on the staff member's file. The Headteacher (or Deputy Headteacher in her absence, will determine the correct course of action to take which could include:

- Implementing an enhanced programme of online safety training for the individual
- Implementing online safety CPD for the whole or groups of staff
- Issuing reminders or updates to staff
- Referring the incident to the LADO
- Disciplinary proceedings.

Breaches by pupils

Any breach of online safety practice by staff will be addressed through the application of the appropriate policy: Child Protection and Safeguarding Policy, Anti-Bullying Policy and Behaviour Management Policy (not an exhaustive list).

Any breach of online safety practice will be recorded on CPOMs. Staff, through reference to the D/DSL, will determine the correct course of action to take which could include:

- Consolidation of online safety education for the individual child/group involved
- Whole cohort online safety revision/consolidation learning
- Engagement of parents and carers
- Sharing of resources to parents and carers and/or children
- Inviting individual parents and carers or the parents of a group or the whole cohort to a meeting to address specific online safety issues
- Engaging an outside speaker to present information to children
- Engaging an outside speaker to present information to parents and carers
- Review of systems in place to safeguard against online safety issues
- Review of staff CPD

Training

Safeguarding, online safety and acceptable use of ICT and the internet form part of the induction process for any new member of staff.

All members of staff and governors receive annual Safeguarding Training, which includes the Staff Code of Conduct and online safety issues.

Safeguarding updates are shared with staff as appropriate in response to events that occur or new developments. Weekly safeguarding updates are shared with staff through the staff meeting and/or through the weekly staff briefing. Online safety forms a natural part of these updates.

The D/DSLs attend termly Safeguarding Briefings from an external safeguarding consultant, which highlight any current national or local online safety issues and how they sit within different aspects of safeguarding.

The D/DSLs attend termly Local Authority safeguarding briefings which give updates on local and national online safety issues.

Monitoring

The impact of the online safety curriculum is monitored through work scrutiny and gathering of pupil voice by the Computing Lead and by the PSHE Lead as part of subject area monitoring processes. The D/DSL may also gather pupil voice through safeguarding monitoring and will pay particular attention to children in the vulnerable groups identified above.

Impero alerts are responded to by the Headteacher and/or Deputy Headteacher on a daily basis. The procedure followed is detailed in Appendix 1. Any alerts that are deemed to be genuine are recorded either on staff files or on CPOMs. Staff files are monitored each time a concern is raised.

E-safety incidents are monitored half termly by the D/DSLs and SENDCo as part of the regular safeguarding monitoring process. This includes monitoring individual children who are identified as being involved with online safety incidents and groups of vulnerable children. Online safety incidents are also monitored for any emerging trends that may indicate the need for further online safety work or an emerging problem.

Review of the policy

This policy will be reviewed annually inline with the Child Protection and Safeguarding Policy review schedule.

Appendix 1
IT Alert Procedures

1. Systems to monitor appropriate use

All devices (PCs, laptops and ipads) that belong to school have the monitoring system *Impero* installed. Every time something with the potential to stem from inappropriate use of the device is displayed on the screen, an Impero alert is created. The alert is emailed to the Head Teacher (Designated Safeguarding Lead, DSL) and the Deputy Head Teacher (Deputy Designated Safeguarding Lead).

2. Content of the Impero Alert

The alert that is received includes:

- A screenshot of the display on the device
- The name of the user (if the device is a pupil device, this can be the number of the device)
- The ID code of the device
- The time the alert was triggered
- The reason the alert has been triggered (e.g. 'Race & Religious Hatred'; 'Adult Content', etc)
- A quote of the information that triggered the alert (e.g.'rifle')

It should be noted that the system is very sensitive and innocent things can trigger an alert to be sent, for example 'your hard work' contains 'ur hard' which would trigger the alert under bullying; or recording of other safeguarding concerns can necessarily include words which would trigger the alert.

3. Procedure to follow on receiving an alert

On receiving an alert, the following procedure will be implemented:

- The Headteacher/Deputy Head will read the alert notification and establish whether the concern is genuine or whether the alert has been triggered for an innocent reason. It may be necessary for the screenshot to be examined to fully determine this.
- If the alert has been triggered for an unnecessary (innocent) reason, the alert can be deleted.
- If the alert has been triggered for a genuine reason, the Headteacher/Deputy Head will determine whether the concern has been generated by a member of staff or on a pupil device.

If the alert has been triggered for a genuine concern and generated by a **member of staff**:

- The investigation of the alert will be conducted by the Head Teacher, or in her absence, the Deputy Head Teacher.
- Every effort will be made to determine the identity of the member of staff. This will usually be straight forward as the name of the person the device has been allocated to is included in the alert. However, the Headteacher should determine that they

have identified the correct person by looking at the screenshot and establishing what the device was being used for and the time the alert was generated.

- The Headteacher will arrange an informal meeting with the member of staff to establish any necessary further details regarding the alert. If at any point, the Head Teacher feels there is the potential for formal action to be necessary, the Head Teacher will stop the informal meeting and implement the Disciplinary Policy or Allegations Against a Member of Staff Policy or Safeguarding Policy as necessary. Procedures and record-keeping will follow those laid out in these policies.
- If the concern does not require implementation of the above policies, the meeting with the Headteacher and member of staff will identify why the alert presented a concern, why this is not acceptable and the risks it poses to pupils and the member of staff, and a reminder of the relevant Child Protection and Safeguarding Policy, Staff Code of Conduct Policy, Acceptable Use of IT Policy or any other relevant Policy/procedure for future use of IT. A Low Level Concerns Form will be completed and saved in the staff member's file.
- The Head Teacher (or Deputy Head in her absence), will review whether further training needs to be delivered to all or a specific group of staff.

If the alert has been triggered for a genuine concern and generated by a **pupil**:

- The Head Teacher may conduct the investigation herself, or refer the investigation to a (D)DSL.
- All attempts will be made to ascertain who was using the device when the alert was triggered. This may be through tracking who has used a specific device at a specific time, looking at information on the screen, such as the program being used or the work being completed, or looking at user names, etc displayed on the screen.
- If the pupil who triggered the device can be identified, a DSL will speak with the pupil to establish if there is any further information relevant to the alert. This could include, but is not limited to: Has any 'sexting' taken place? Is the child bullying/being bullied? Is there a concern regarding potential grooming/County Lines/Serious Crime/Gang involvement? Is there a concern regarding the child's mental or physical health? Are there other safeguarding elements involved?
- The DSL will also seek to establish whether the alert indicates the involvement of any other children. In the event that other children are involved, the (D)DSL will include these children in their response.
- The DSL will decide whether the incident requires the Child Protection and Safeguarding Policy or the Behaviour Management Policy (or both) to be implemented and will respond in accordance with the relevant policy(ies). Any response will be in-line with all other relevant policies, for example, the Anti-Bullying Policy or Mental Health and Wellbeing Policy.
- Where appropriate, the pupil's parents will be informed, with details of the concern. Strategies to support the online safety of their child at home will be shared.
- The DSL will, in conjunction with other relevant staff (Computing Lead, class teacher, Care Club Manager, etc) decide whether further learning with regard to online safety or other e-safety needs to be delivered to the individual, groups or classes of pupils.

- All genuine concerns triggered by an Impero alert and the resulting actions will be recorded on CPOMs in accordance with the Child Protection and Safeguarding Policy and/or the Behaviour Management Policy.
- The Head Teacher will review whether any additional response to the incident needs to be actioned, for example, information sheet to be communicated to parents, parent workshop on e-safety, engaging the support of outside agencies, such as the PCSO (Police Community Support Officer), etc.

7 Pupil Use of IT devices

Each device has an individual ID code that takes the form of: STM-LT-ST-0??
To aid in identifying which pupil has triggered an alert when using a school device, the following will take place:

- If a child has been lent a device to use at home (for example, to support remote education), the device ID code will be recorded against the pupil's name on the lending record.
- If a child frequently uses a device during lessons, for example, to access Clicker to support with writing, the child will record the device number in their book under the date/title. When a child frequently uses an IT device, the child will often aim to use the same device to simplify accessing the work.
- When individual children are using devices, for example if a whole class is using IT devices for a computing lesson, a record of who is using which device will be made by the class teacher and kept for 48 hours after the lesson has taken place.

Appendix 2

St Thomas More Catholic Primary School
Pupils' Acceptable Use of Technology

I will always:

- Behave kindly and appropriately when online, including using appropriate language.
- If I see, hear or know of something online that I think might be wrong, or makes me feel upset, I will tell a trusted adult, e.g. a teacher, learning assistant or my parent or carer.
- Keep information about myself and others (e.g. name, age, school, address, etc) safe and not share it online.
- Only use the apps, websites, programs, etc that I am supposed to be using.
- Look after school devices.
- Use school devices and not my own device in school.
- Work using the online safety learning and tools that are in school to keep me safe.
- Use online information to find things out but not copy off the internet.

I will never:

- Be unkind or bully anyone.
- Do anything I know is wrong.
- Do anything that is against the law.
- Try to install anything when I'm using a school device.
- Delete anything without permission when I'm using a school device. If I do it accidentally, I will immediately stop and tell a trusted adult.