ST TERESA of CALCUTTA
Catholic Academy Trust

Central Trust Digital Safeguarding Policy

Policy Level	Trust/Statutory	**Ref No**	SF05
Approved by	CSEL	**Approved date**	19.01.25
Responsibility	PB	**Next review date**	Autumn 2025
Published location	STOC Shared Policy Folder		
Version number	**Date Issued**	**Author**	**Update Information**
1.1	12.09.23	PB	Updated Safeguarding points

Our Mission and Values

Our Mission

Our Trust Mission is simple, it is to make Christ known, making lives better for our communities, our children, and our young people.

Commitment to Equality

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation.

We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

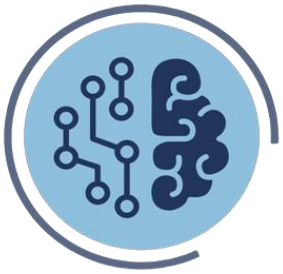
Our Values

Hope

Inspired by St Teresa of Calcutta, we are people of hope. We have a complete belief in the future we will build together. By offering our children, staff and schools' opportunities to grow and flourish, we make aspiration and ambition a reality. Our people, just like St Teresa are relentless and fiercely ambitious. We will always reach for that which seems to be just out of our grasp.

Courage

As modelled for us by St Teresa of Calcutta, we will have the courage to do what is right. As a community, we will not shy away from making decisions that ensure our communities thrive. We will be brave in our actions. As a truly Catholic organisation this courage will be most apparent in how we collectively support the most vulnerable.



Innovation

St Teresa of Calcutta changed the world. Together, we will always be pursuing new ideas and best practice in all areas of our work. We will prepare our children and young people for the world that awaits them. A world which they will shape and change.

Contents Page

St Teresa of Calcutta Catholic Academy Trust Digital Safeguarding Policy September 2024

This Central Trust Policy is designed to ensure that all staff know and understand how we safeguard children in relation to digital safety. It demonstrates how we meet the Department for Education 'Meeting Digital Standards in Schools and Colleges' and Keeping Children Safe in Education 2024. It should also be read in conjunction with Central Trust Guidance for Safe Working Practice (Code of Conduct).

It is applicable for all staff who work within the organisation including those who may be contracted in or enrolled as an apprentice. It outlines the expectations for central staff and the expectations for all schools, staff, professionals and volunteers within the schools.

This document provides a framework for ensuring consistency, accountability, support and knowledge transfer and identifies the key controls across the Catholic Academy Trust. This document will be read in conjunction with other key policies held centrally and those policies held at individual academy level. It is developed in line with the UK Council for Internet Safety, Digital Resilience Framework.

As a values driven organisation, whose mission is to Make Christ Known and ensure we are making lives better for our communities, our children and young people and all of our stakeholders, the importance of Safeguarding is paramount to us. It is an area that underpins all that we do.

Part B of this policy includes our social media Policy.

1. Purpose of the document

1.1 To ensure that all staff know and understand the importance of Digital Safeguarding within St Teresa of Calcutta Catholic Academy Trust and that promoting the welfare of children in our care, including online is everyone's responsibility.

1.2 To ensure that all staff within St Teresa of Calcutta Catholic Academy Trust understands their roles when using digital technology either as a teaching and learning tool and/or when addressing issues that may arise online.

1.3 To ensure that all staff know that safeguarding is effective when there is an ethos in each school where children feel secure, are encouraged to talk, are listened to and know that there are adults in the school who they can approach if they are worried or listened to. To ensure that all staff know their role in this, particularly in relation to digital safeguarding and online activity.

1.4 To ensure that all staff know that leaders within St Teresa of Calcutta Catholic Academy Trust will take action when Child Protection and Safeguarding policy and procedure is not followed or as outlined within Guidance for Safe Working Practice (Code of Conduct).

2. Introduction and Safeguarding Statement of Intent:

In line with Keeping Children Safe in Education 2024, Safeguarding is:

- Protecting children from maltreatment, whether that is within or outside the home, including online
- Providing help and support to meet the needs of children as soon as problems emerge
- Preventing the impairment of children's mental and physical health or development
- Ensuring that children grow up in circumstances consistent with the provision of safe and effective care, and
- Taking action to enable all children to have the best outcomes.

Child protection is part of this definition and refers to activities undertaken to prevent children suffering, or being likely to suffer, significant harm or exploitation.

Safeguarding and promoting the welfare of children is everyone's responsibility. No single practitioner can have a full picture of a child's needs and circumstances. Everyone who comes into contact with children and their families has a role to play in identifying concerns, sharing information and taking prompt action.

In order to fulfil this responsibility effectively, all practitioners should make sure their approach is child centred. This means that they should consider, at all times, what is in the best interests of the child.

St Teresa of Calcutta Catholic Academy Trust is committed to safeguarding children and young people, and we expect everyone who works in our schools and Central Trust to share this commitment. We want all our children to feel safe and cared for in our schools and to know that this is a safe place and there are trusted adults to whom they can turn. We want all the adults who work for us to be fully equipped to fulfil their duty of care towards promoting the safeguarding and welfare of all our children.

As public servants, our responsibility for all staff to safeguard children and promote their welfare is enshrined in law; as practitioners within the Catholic Education Service there is an additional duty on us to care for the poor and educate those who are socially, academically, physically or emotionally disadvantaged. This incorporates safeguarding children so that they are protected from maltreatment; that we take action that prevents impairment of their mental and physical health and development; that we ensure that children grow up in circumstances consistent with the provision of safe and effective care; and that we take action to enable all children to have the best outcomes.

Children at our schools are taught about how they can keep themselves and others safe, including online. This Central Digital Safeguarding Policy provides information

on how we filter and monitor our online activity centrally to keep children safe and our expectations for schools. We expect our schools to teach children how to keep safe in an age-appropriate way and monitor this through our School Improvement offer and professional networks. We expect our staff to be sensitive to the specific needs and vulnerabilities of individual children who are victims of abuse, children with special educational needs or disabilities and children who need a social worker. We expect our DSLs and leadership teams to adapt practice to support children in relation to safeguarding.

Our practice across schools includes an expectation to being alert to those children who are absent for prolonged periods, have sporadic attendance and may miss part of the school day so that we fulfil our duty early to help prevent the risk of a child missing education in the future. We will provide guidance and support.

We recognise the impact of wider environmental factors in a child's life that may be a threat to their welfare and/or safety (extra-familial harms[1]) and aim to be outward facing so that we can effectively assess the risks and issues in the wider community when considering the well-being and safety of our pupils. To do this our Head of Safeguarding will engage with Safeguarding partnership boards and keep up to date with national agendas.

Adults across our schools and in the Central Trust take all welfare concerns seriously and encourage children and young people to talk to us about anything that worries them. In order to help young people achieve this, school leaders should foster an open, honest and transparent culture whereby children and staff feel listened to and that their concerns are acted upon.

All adults across our schools know that Safeguarding is a non-negotiable with Trust leaders and school leaders and we are vigilant to Safeguarding risks.

All adults will always act in the best interests of the child.

[1] KCSIE 2024 Paragraph 21 states: All staff, but especially the designated safeguarding lead (and deputies) should consider whether children are at risk of abuse or exploitation in situations outside their families. Extra-familial harms take a variety of different forms and children can be vulnerable to multiple harms including (but not limited to) sexual abuse (including harassment and exploitation), domestic abuse in their own intimate relationships (teenage relationship abuse), criminal exploitation, serious youth violence, county lines and radicalisation.

3.0 Leadership Structure, Roles and Responsibilities:

3.1 The Board of Directors

The Board of Directors hold ultimate accountability for safeguarding, including digital safeguarding, across all academies within St Teresa of Calcutta Catholic Academy Trust.

3.1.1 The Chair of the Trust ensures that Safeguarding is on the agenda of every Trust Board Meeting with the Head of Safeguarding reporting on this item. This includes Digital Safeguarding.

3.1.2 There is a named Director for Digital Safeguarding who reports to and acts on behalf of the Trust Board.

3.1.3 The Head of Safeguarding works closely with the Chief Information Officer to understand and provide strategic challenge in relation to Digital Safeguarding.

3.1.4 The named Director is aware of any Digital Safeguarding risks within St Teresa of Calcutta Catholic Academy Trust and works closely with the Head of Safeguarding who is responsible for Safeguarding, to ensure that Safeguarding is high-profile across the trust and that procedures are in place to safeguard children online, including when using new and emerging technologies.

3.2 Central Executive Team

3.2.1 The Chief Information Officer, holds responsibility for the Central Executive Team for Digital Safeguarding, and works in conjunction with the Head of Safeguarding to ensure the Central Executive Team are up to date with new and emerging risks, locally and nationally.

3.2.2 The Chief Information Officer, with the central IT team, are responsible for procurement of IT services, including learning platforms and Management Information Systems across the Trust and ensuring that third party managed service providers are aligned with the security policies held by the Trust.

3.2.3 The Chief Information Officer will procure relevant hardware and software for use across schools.

3.2.4 The Chief Information Officer will ensure that the IT Security Policy is followed by the Central Services Team and across all schools, and that any breaches are reported directly to her.

3.2.5 The Chief Information Officer will undertake at least an annual review of filtering and monitoring systems in each of the schools. Where a breach has taken place, or concerns have been raised by staff, this may constitute an immediate review. Other triggers may be a change in working practice, i.e. remote learning and/or a change in technology.

3.2.6 The annual review will be conducted by the Chief Information Officer (lead), Head of Safeguarding, school DSL and IT lead. It will be recorded for reference and available for review by local governing bodies and The Board of Directors.

3.2.7 The review will include:

- The risk profile of pupils in the school, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- What the filtering system currently blocks or allows and why
- Any outside safeguarding influences, such as county lines
- Any relevant safeguarding reports
- The digital resilience of your pupils
- Teaching requirements, for example, the RHSE and PSHE curriculum
- The specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- What related safeguarding or technology policies you have in place
- What checks are currently taking place and how resulting actions are handled

3.2.8 The review will ensure that decisions will be made based on each individual school, this might include changes in roles and responsibilities, training of staff, curriculum and learning platforms, any changes to procurement practice, increased checks and reviews, effectiveness of monitoring strategies.

3.2.9 The Chief Information Officer will also procure external review across the Catholic Academy Trust in line with growth and onboarding strategies.

3.2.10 As the Trust grows and develops, external review of schools as part of due diligence may form part of the onboarding process. This will be in line with what is known about current practice locally and support given/not given by Local Authority teams.

3.2.11 The Chief Information Officer will ensure that the Central IT team will undertake more regular local checks with IT leads and DSLs in school to ensure that:

- System set ups have not been changed or deactivated.
- That a range of school owned devices are functioning effectively
- Sample checks of teacher, pupil and guests demonstrate filtering working effectively.

3.2.12 The Chief Information Officer will ensure that our filtering system:

- Is a member of Internet Watch Foundation (IWF)
- Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Blocking access to illegal content including child sexual abuse material (CSAM)
- Includes all users[2], including guest accounts, school owned devices and devices using the school broadband connection
- Filters all internet feeds, including any backup connections
- Be age and ability appropriate for the users, and be suitable for educational settings
- Handle multilingual web content, images, common misspellings and abbreviations
- Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them

[2] All users must use the provided usernames and email addresses from the Central Team. Stoccat.org.uk will be the email address all staff, including local governing bodies.

- Provide alerts when any web content has been blocked
- Enables us to identify device name or ID, IP address, and where possible, the individual; the time and date of attempted access; the search term or content being blocked.

3.2.13 The Chief Information Officer will ensure that a range of monitoring systems are strong in each school including:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

3.2.14 The Chief Information Officer will ensure that training is provided so that staff have the technical expertise in relation to monitoring.

3.2.15 The Chief Information Officer will procure training for specialist staff and ensure, with the Head of Safeguarding, that online Safeguarding training meets the needs of the Trust.

3.2.16 In cases of Bring Your Own Devices (see Section 5), these will be agreed as an exception in writing by the Chief Information Officer.

3.2.17 The Chief Information Officer will ensure that the Cyber security standards are met as part of our Security Policy and that these are regularly reviewed.

3.3 Leadership Teams in School:

3.3.1 The Headteacher should ensure that IT leads in school, including IT technicians and IT teaching and learning leads, understand the requirements in this policy and that they are the day-to-day operations for ensuring the conditions that fall under the remit of the Chief Information Officer are met.

3.3.2 The Headteacher should ensure the DSL understand their responsibilities in relation to filtering and monitoring and acting upon concerns.

3.3.3 The Headteacher will ensure that any request for learning platforms or teaching and learning aids is procured through consultation with the Chief Information Officer and/or their teams so that security can be verified centrally before procurement.

3.3.4 Where the Headteacher requests to deviate from the Bring Your Own Devices (see Section 5) this should be in consultation with the Chief Information Officer with a written record of the consultation and agreement made including reviews.

3.3.5 In line with Safer Recruitment Policy, Headteachers should be aware of their responsibilities in relation to online searches that may be done as part of due diligence checks. Paragraph 226 of KCSIE 2024.

3.3.6 Headteachers should ensure that the curriculum covers online safety, and children are taught how to be digitally resilient.

3.3.7 Headteachers should ensure that all staff have read, understood and signed for Guidance for Safe Working Practice (Code of Conduct) and that staff understand their Digital

Safeguarding responsibility in relation to Section 3.1, 3.2.2, 3.4, 3.7, 3.8, 3.9, 3.11, Section 4.

3.3.8 Headteachers should ensure that all staff have read, understood and signed for Safeguarding and Child Protection Policy and understand their Digital Safeguarding responsibility in relation to Section 3 Child-on-Child Abuse, Section 4 Prevent Duty, Section 6 Online safety, Section 9 Role of the Designated Safeguarding Lead.

3.3.9 Headteachers should ensure that the online safety training is applicable to all staff and that all staff know their responsibility in reporting any online concerns via CPOMS if they:

- See or suspect unacceptable content being accessed.
- Unacceptable content can be accessed.
- Teaching content that could cause a spike in logs.
- Failure or abuse of the system.
- Perceived unreasonable restrictions.
- Abbreviations or misspellings that allows access to unacceptable content.

3.3.10 Headteachers should ensure that all staff know that if there are concerns about sites being blocked that unreasonably impact on their teaching and learning they should notify the Headteacher and/or relevant Curriculum Deputy and IT lead.

3.4 All staff:

3.4.1 All staff should be aware of the four areas of risk in relation to online safety:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

3.4.2 That all staff understand and fulfil their responsibility in relation to Exposure to Inappropriate Images Section 3.4 Guidance for Safe Working Practice (Code of Conduct).

3.4.3 That all staff understand and fulfil their responsibility in relation to Social Contact outside the workplace with families Section 3.7 Guidance for Safe Working Practice (Code of Conduct).

3.4.4 That all staff understand and fulfil their responsibility in relation to Communication with Children and Young People (including the use of Technology) Section 3.8 Guidance for Safe Working Practice (Code of Conduct).

3.4.5 That all staff understand and fulfil their responsibility in relation to The Use of Personal Living Space including the delivery of online learning Section 3.9 Guidance for Safe Working Practice (Code of Conduct).

3.4.6 That all staff understand and fulfil their responsibility in relation to Photography, Videos and other Creative Arts Section 3.11 Guidance for Safe Working Practice (Code of Conduct).

3.4.7 That all staff follow Central Trust Procedure in relation to Acceptable Use and Bring Your Own Devices.

3.5 Local Governing Bodies:

3.5.1 Local Governing bodies have a strategic leadership responsibility for their academy's safeguarding arrangements and must ensure that they comply with their duties under the legislation and their obligations under the Human Rights Act 1988, Equality Act 2010 (including the Public Sector Equality Duty 2011) and their local multi-agency safeguarding arrangements.

3.5.2 Local Governing Bodies should make sure that they have read and understood Part One and Annex B of Keeping Children Safe in Education 2024.

3.5.3 Local Governing Bodies should make sure that at least one governor understands and is responsible for the strategic oversight of Meeting Digital Standards in Schools in their school. This can be the Local Governing Body responsible for Safeguarding.

3.5.4 That at least one governor is Safer Recruitment trained and that when recruitment takes place, they are assured that a member of the panel is Safer Recruitment trained.

3.5.5 Local Governing Bodies should appoint a Safeguarding governor from their team alongside a governor for Looked After children and SEND. This governor will take leadership responsibility for their school's Safeguarding arrangements.

3.5.6 That the Local Governing Body ensures Digital Safeguarding forms part of the annual Safeguarding report, and they are updated termly on any digital safeguarding risks.

3.5.7 That the Local Governing Body follows the expectations in relation to Acceptable Use and Bring Your Own Devices.

4.0 Acceptable User Policies:

4.1 All staff and pupils will be expected to read and sign for an online Acceptable User Policy before accessing St Teresa of Calcutta hardware and software.

4.2 All pupils and staff will have centralised sign in and be expected to keep their passwords safe. For those in Early Years and Key Stage 1, sign in to access technology will be agreed with the Central Team and may be different to those in Key Stage 2, 3 and 4.

4.3 All staff will be expected to use Trust email addresses for communication. This includes Local Governing Bodies and The Board of Directors.

4.4. Any breach of the Acceptable User Policy could result in that pupil's or member of staff's access to the technology being denied.

5.0 Bring Your Own Devices

5.1 The Trust provides all hardware for staff and pupils to use that complies with our Security Policy.

5.2 The Trust does not endorse Bring Your Own Devices with these exceptions:

- Local Governing Bodies may use their own devices but are expected to communicate via STOCCAT email addresses. Personal email addresses cannot be used. Documentation in relation to school business should not be stored on their personal devices.
- Consultants, advisors may use their own devices but should access the school's Wi-Fi through a guest account.
- The use of mobile phones by pupils in any of our schools are not advised. We recognise however that schools may be at different points in this and, as they work towards mobile phones by pupils being phased out, they should discuss this with the Chief Information Officer and outline this in the Safeguarding and Child Protection Policy Section 6.
- Some individual pupils may need to use a mobile phone as part of their EHCP or IHCP, in these cases this will be discussed with the SENCO and DSL and recorded.

Section B

Social Media Policy

1. Policy Statement:

1.1 The widespread availability and use of social media applications brings opportunities to communicate in new and innovative ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our Trust schools, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children and young people. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of the Trust.

2. Scope and Purpose

2.1 The purpose of the policy is to:

- Protect the Trust from legal risks.
- Ensure that the reputation of the Trust, its staff and Local Governing Bodies are protected.
- Safeguard all children.
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the Trust.

2.2 Definitions and Scope Social networking applications include, but are not limited to:

- Blogs.
- Online discussion forums.
- Collaborative spaces.
- Media sharing services.
- 'Microblogging' applications.
- Online gaming environments - Examples include X formerly Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr, and comment streams on public websites such as a newspaper site.

2.3 Many of the principles of this policy also apply to other types of online presence. All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation as well as other legislation. They must also operate in line with the Trust's Guidance for Safe Working Practice (Code of Conduct), Digital Safeguarding Policy, Safeguarding and Child Protection Policy. Within this policy there is a distinction between the use of trust-approved social media for educational purposes, and personal use of social media.

3. Staff Personal Use of Social Media:

3.1 Guidance for Safe Working Practice (Code of Conduct) outlines very clearly the expectations in relation to communicating with families and children. A summary of this is included below:

- Trust staff will not invite, accept or engage in communications with parents/carers or children from Trust school communities in any personal social media whilst in employment at the Trust.
- Any communication received from children on any personal social media sites must be reported to the Designated Safeguarding Lead.
- If any member of staff is aware of any inappropriate communications involving any child on any social media, these must immediately be reported as above.
- Members of staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the Trust's school communities on Trust business must be made from an official Trust email account.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the Trust and members of its community on any social media accounts.
- Staff are also advised to consider the reputation of the Trust in any posts or comments related to the Trust on any social media accounts. Any posts or comments that bring the Trust's name into disrepute could result in disciplinary action.
- Staff should not accept any current student of any age or any ex-student of the Trust under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

4. Trust Approved Use of Social Media:

4.1 All schools are encouraged to maintain a regular social media presence with a view to keeping family members and communities up to date on school developments and important news. When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff and ideally should be linked to an official Trust email account. Trust social media accounts must only be set up further to approval by SLT.
- The identity of the site should be notified to the appropriate member of SLT before access is permitted for students.
- The content of any Trust-approved social media site should be solely professional.
- Staff must not publish photographs of children without the consent of parents/carers, identify by name any children featured in photographs, or allow personally identifying information to be published on Trust social media accounts.
- Care must be taken that any links to external sites from the account are appropriate and safe.

- Any inappropriate comments on or abuse of Trust-approved social media should immediately be removed and reported to a member of SLT.
- Staff should not engage with any direct messaging of students through social media where the message is not public.

4.2 Where possible, social media handles will be in the format @schoolname, in lowercase.

4.3 All schools will post at least 3 times per week, showcasing the work that is going on in their schools.

4.4 All schools will use social media to promote opening evenings, parents' evenings, parish events and keep communities up to date on school developments and important news.

4.5 The SLT within each school will be responsible for quality assuring the content posted on their social media platforms and ensuring it does not bring the school or the Trust into disrepute.

5.0 Pupil Use of Social Media:

5.1 Bring Your Own Devices in the Digital Safeguarding Policy (Section 5) outlines the expectations in relation to this. Our filtering system will block access to social media sites. Pupils will not be able to access the school wi-fi system.

5.2 Pupils will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Pupils are only permitted to be affiliates of school social media accounts. Where a pupil or parent attempts to "friend" or 'follow' a staff member on their personal account, it will be reported to the headteacher.

5.3 Pupils will not post any content online which is damaging to the school or any of its staff or pupils. Pupils will not post anonymously or under an alias to evade the guidance given in this policy.

5.4 Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil's age.

5.5 If inappropriate content is accessed online on school premises, it will be reported to the DSL as outlined in this policy and in the case of indecent images of children reported immediately to the Headteacher.

5.6 Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to school-based sanctions.

6.0 Glossary of Terms

The following definitions are crucial to understanding our Social Media Policy. This list is not exhaustive.

Social media means any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Social media includes but is not limited to, online social forums such as X – formerly Twitter, Facebook and LinkedIn and also covers blogs,

chat rooms, forums, podcasts and video image-sharing websites such as YouTube, Flickr, Reddit, Instagram, Snapchat, WhatsApp, Pinterest and Tumblr.

Staff/adults working in school means all members of staff and those who work on a self-employed basis. It also includes trainee teachers, other trainees and apprentices, volunteers, agency staff, external consultants and school Local Governing Bodies/The Board of Directors.

Information means all types of information including but not limited to, facts, data, comments, audio, video, photographs, images, texts, e-mails, instant messages and any other form of online interaction.

Inappropriate information means information as defined above which any reasonable person would consider to be unsuitable or that brings into question the professional integrity of the adult, given their position within the school. (See also, Guidance for Safe Working Practice – Code of Conduct).

Trust school communities mean the school, its pupils, all adults working in school (as defined above) parents/carers of pupils, former pupils, the Local Authority, the Diocese and any other person or body directly or indirectly connected with the school.