St. Theresa's Catholic Primary School

Online Safety Policy

"We learn together, we play together, we pray together, we grow together in the love of God"

St.Theresa's
Catholic Primary School

Validation grid

Title	Online Safety Policy
Author	Barbara Costa
Associate Author	LGfL
Committee	Wellbeing
Target Audience	All Staff, parents, Governors
Stakeholders Consulted	Staff and Governors
Curriculum / Non Curricular	Non Curricular
Associated Policies / Documents	Staff Code of Conduct, Child Protection and Safeguarding Policy, Data Protection Policy, Behaviour Policy, Anti-Bullying Policy, Freedom of Information Publication Scheme, PSHE Policy, Relationships and Sex Education Policy, Keeping Children Safe in Education 2025
New Policy or Review of Existing Policy	Review
Date of Submission	November 2025
Date for Review	November 2026

Headteacher Barbara Costa Barbara Costa

Chair of Governors Fiona Kerin

Introduction

Key people / dates

St. Theresa's	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Barbara Costa
	Deputy Designated Safeguarding Leads / DSL Team Members	James Troy Barbara Folan
	Link governor for safeguarding and webfiltering	Jane Goring
	Curriculum leads with relevance to online safeguarding and their role	PSHE: Carmen Decuseara RSE: Barbara Costa Computing: Jessica Porcu
	Network manager / other technical support	ICT Inspire

Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Unkind comments on gaming apps
- Unkind comments on messaging apps
- Children attempting to access inappropriate websites
- Children playing online late at night

Contents

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all St. Theresa's School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the Executive Headteacher will handle referrals to the LA designated officer (LADO).

Scope

This policy applies to all members of the St. Theresa's community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Education and curriculum

The school recognises the opportunities and benefits to children too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships and Sex Education (RSE)
- Personal, Social and Health Education (PSHE)
- Computing
- Citizenship

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, generative AI tools etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation,

misinformation, and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

At St. Theresa's, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to look closely at areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. S safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Data Protection Policy
- Acceptable Use Policies (see appendices)

This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead as soon as possible on the same day – this includes any concerns raised by the filtering and monitoring systems.

Any concern/allegation about staff misuse is always referred directly to the Executive Headteacher, unless the concern is about the Executive Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline 0808 800 500.

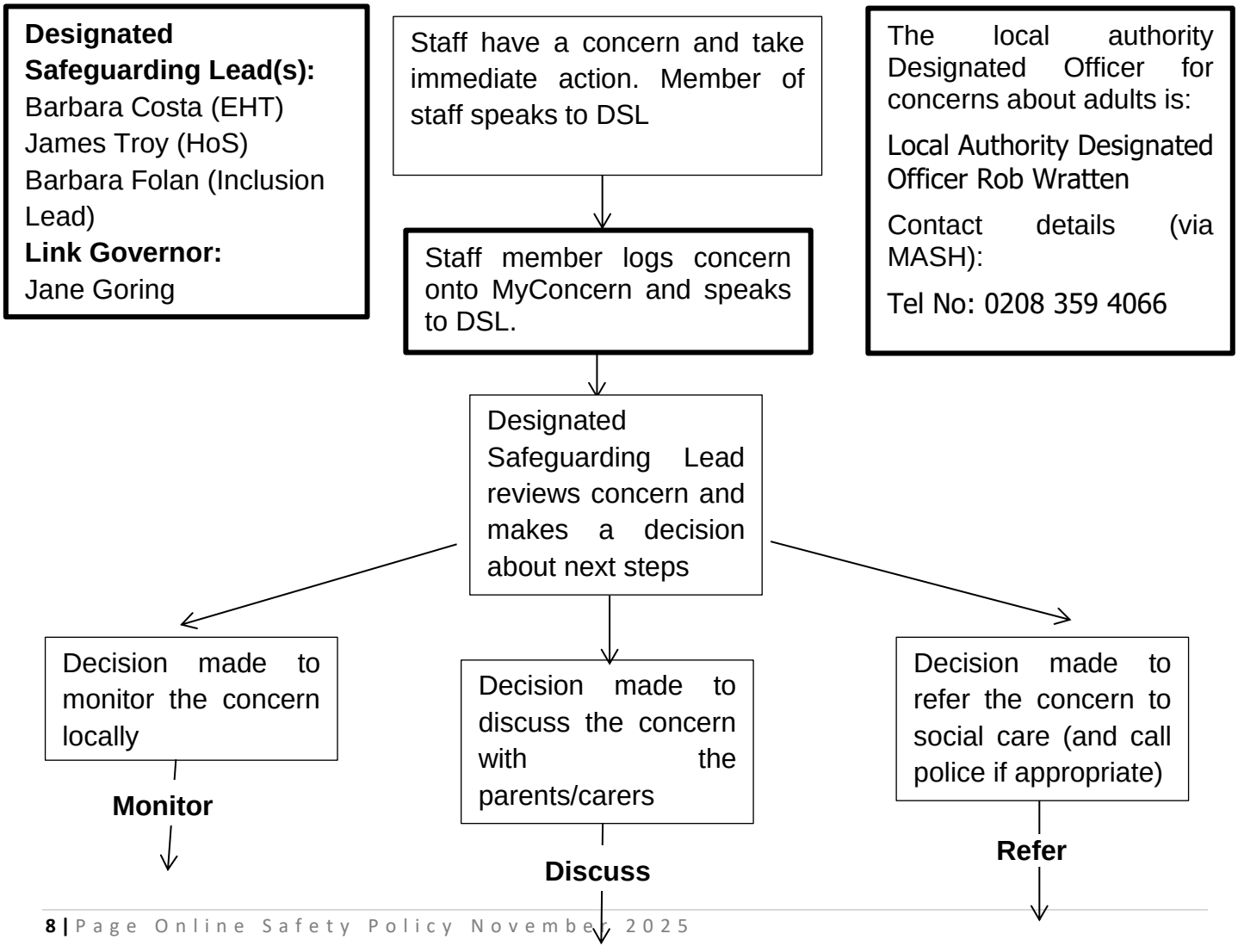
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

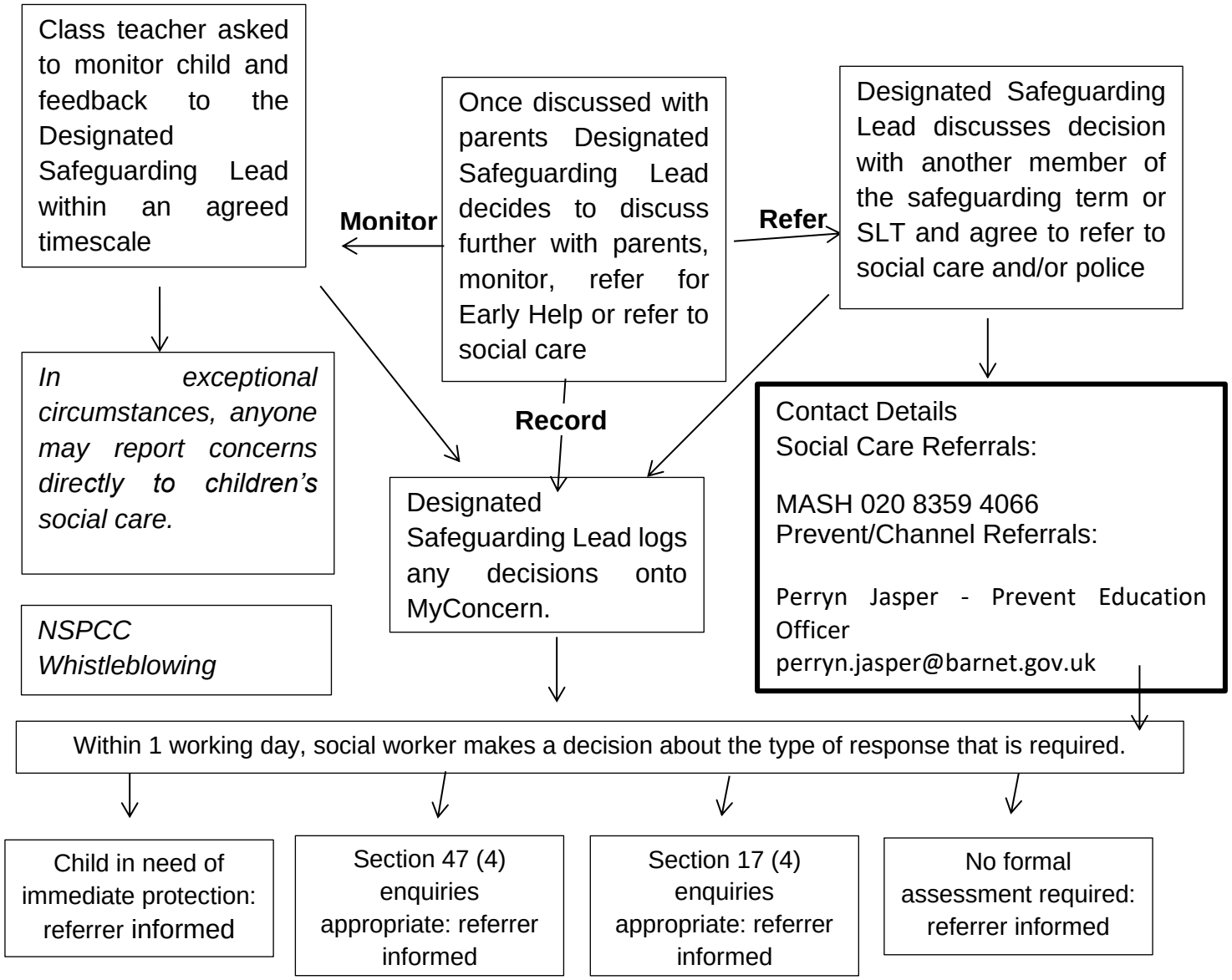
We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school will evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc. and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is taken from the school's Child Protection and Safeguarding Policy and outlines what action is taken where there are concerns about a child; online safety concerns are no different to any other safeguarding concern.





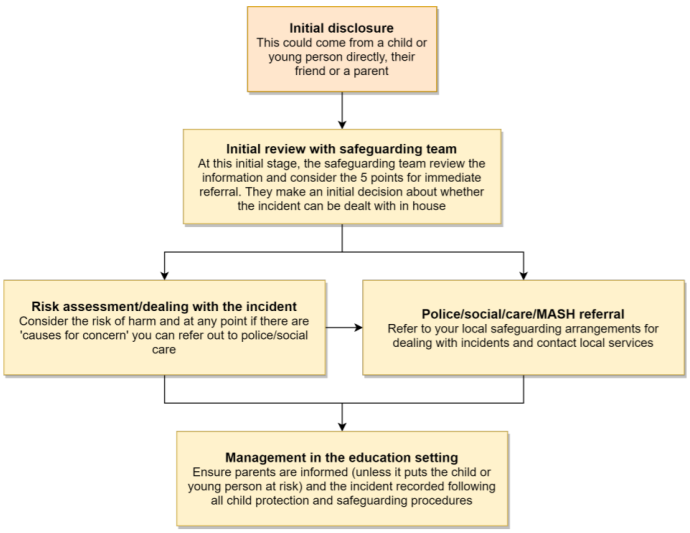
Nudes – sharing nudes and semi-nudes

This school will refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

Whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying (which may also be referred to a cyberbullying) including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. The school's Anti-Bullying Policy can be found on the school website: https://www.st-theresas.barnet.sch.uk/school/policies/

The school is aware that sometimes fights are filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. Staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy [please see appendices] as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the Staff Code of Conduct and the Staff Handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the St. Theresa's community. These are also governed by Acceptable Use Policies.

Breaches will be dealt with in line with the school Behaviour Policy (for pupils) or Code of Conduct/Disciplinary Policy (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, St. Theresa's will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's Data Protection Policy which can be found on the school website: https://www.st-theresas.barnet.sch.uk/school/policies/

Data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of myUSO to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

The Designated Safeguarding Lead has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via email or by logging onto MyConcern and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

The DSL checks filtering reports and notifications half-termly and takes any necessary action as a result. At St. Theresa's our monitoring plan includes:

- monitoring devices using device management software (senso)
- in-person monitoring in the classroom
- network monitoring using log files of internet traffic and web access.

At St. Theresa's:

- web filtering is provided by LGfL Webscreen 3 on school site and for school devices used in the home
- changes can be made by the ICT Inspire staff
- overall responsibility is held by the DSL with support from members of the SLT
- technical support and advice, setup and configuration are from ICT Inspire staff
- regular checks are made half termly by ICT Inspire Staff to ensure filtering is still active and functioning everywhere. These are evidenced in the log book.
- an annual review is carried out
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

- Pupils at this school communicate with each other and with staff using Seesaw.
- Staff at this school use the email system provided by LGfL for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with school staff, parents and external organisations. Staff are not permitted to use the school email to communicate with the pupils.
- Staff at this school use MyUso and Egress to communicate sensitive data.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Executive Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Executive Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements (see appendices), Behaviour Policy and Staff Code of Conduct (https://www.st-theresas.barnet.sch.uk/school/policies/).
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy (https://www.st-theresas.barnet.sch.uk/school/policies/) and only using the authorised systems mentioned above.
- Staff should avoid using the email system for personal use. Staff should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Use of generative AI

At St. Theresa's, we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- Staff are permitted to use AI to assist with planning.

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. St. Theresa's has a clear data protection policy which staff, governors and volunteers must follow at all times: https://www.st-theresas.barnet.sch.uk/school/policies/.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to James Troy.

The site is hosted by Indigo Tree.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc. that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At St. Theresa's members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Our SM presence

St. Theresa's works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

James Troy is responsible for managing our Instagram and Twitter accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure (https://www.st-theresas.barnet.sch.uk/school/policies/) should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email, Teachers2Parents and Seesaw are the official electronic communication channels between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

Pupils/students are not allowed to be 'friends'* with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video [this links to the section in this document) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy: https://www.st-theresas.barnet.sch.uk/school/policies/

Device Usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils/students** in Y5 and Y6 who walk to and from school independently are allowed to bring mobile phones in for emergency use only. Upon arrival at school, the phone must be given to either the office staff, or the class teacher. The phone will be returned at the end of the day. Pupils are not permitted to use their phones during the school day.
  Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions in line with the School Behaviour Policy (https://www.st-theresas.barnet.sch.uk/school/policies/). Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in

a professional capacity. Staff mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances. Members of staff are strictly prohibited from allowing children to use mobile phones or a personally-owned device as part of an educational activity.

- Staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then use of their mobile phone will be permitted. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Executive Headteacher should be sought (the Executive Headteacher may choose to delegate this) and this should be done in the presence of a member of staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page 17. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Use of school devices

- **Pupils/students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network
- All internet traffic is monitored
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files/drives. Internet traffic is monitored.
- **Parents** can access the guest wireless network but have no access to networked files/drives. Internet traffic is monitored.

Trips / events away from school

For school trips/events away from school, teachers may use their personal phone in an emergency; they will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

The school also uses Texting to Parents.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy (https://www.st-theresas.barnet.sch.uk/school/policies/).

Appendix I – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the "All Staff" section as well as any other relevant to specialist roles

Roles:

- All Staff
- Executive Headteacher
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the staff code of conduct/handbook (https://www.st-theresas.barnet.sch.uk/school/policies/) and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about over-blocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Executive Headteacher – Barbara Costa

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding

- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Barbara Costa

Key responsibilities (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE
- Take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.

- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - This must include filtering and monitoring and help them to understand their roles
    - all staff must read KCSIE Part 1 and all those working with children also Annex B
    - cascade knowledge of risks and opportunities throughout the organisation
- Ensure that ALL governors undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school
- Work with the Executive Headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends.
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSE guidance and beyond, in wider school life
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP and those hired by parents.

Governing Body, led by Online Safety / Safeguarding Link Governor – Jane Goring

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and Executive Headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

PSHE / RSE Lead/s – Carmen Decuseara and Barbara Costa

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.

Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."

- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age-appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" to complement the computing curriculum.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.
- Note that an RSE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – TBC

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/other technical support roles – ICT Inspire

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.).
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy is up to date, easy to follow and practicable

Data Protection Officer (DPO) – Chorus Advisors

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Appendix II: Key Stage 1 Pupil Acceptable Use Policy

My name is _____

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:	✓
1. I only **USE** devices or apps, sites or games if I am allowed to	
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused	
3. I look out for my **FRIENDS** and tell someone if they need help	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I **KNOW** that online people aren't always who they say they are and things I read or see are not always **TRUE**	
6. Anything I do online can be shared and might stay online **FOREVER**	
7. I don't keep **SECRETS** 🚫 unless they are a nice surprise	
8. I don't have to do **DARES OR CHALLENGES** ❌, even if someone tells me I must. Sometimes these can be dangerous.	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I always check before **SHARING** my personal information or other people's stories and photos	
11. I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school

_____ at home

_____ at _____

Appendix III: Key Stage 2 Pupil Acceptable Use Policy

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

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to. If not sure, I will ask.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it may be hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. ***If I make a mistake I don't try to hide it but ask for help.***
12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about. I check with a trusted adult before I chat with anyone for the first time, even if they are a 'chatbot'.
13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
23. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
24. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
25. ***I am part of a community*** – I do not say mean things, make fun of anyone or exclude them because they are different. If I see anyone doing this, I tell a trusted adult and/or report it. I talk to others online how I would like to be spoken to.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see, and I know which sites to trust, and how to double check information I come across. I will not copy anything without permissions. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult: at school that might mean _____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline and use the classroom worry box.

Signed: _____ Date: _____

Appendix IV: Parent/Carer Acceptable Use Policy

Background

We ask all children, young people and adults involved in the life of St. Theresa's to read and sign an Acceptable Use* Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP which has been sent home.

We tell your children that **they should not behave any differently when they are out of school or using their own device or on a home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read St. Theresa's' full Online Safety Policy https://www.st-theresas.barnet.sch.uk/school/policies/) for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc.). If you have any questions about this AUP or our approach to online safety, please speak to Barbara Costa (tel: 020 8346 8826 email: office@sttheresas.barnetmail.net).

What am I agreeing to?

1. I understand that St. Theresa's uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I will support my child to follow the school's policy regarding bringing devices to school. Only Y5 and Y6 pupils are permitted to bring mobile phones to school and must be handed to the office,

or class teacher upon arrival. The mobile phones will be returned to the child at home time. Pupils are not permitted to use their phones during the school day.

7. I understand that my child might be contacted online on Seesaw by school staff and only about their learning, wellbeing or behaviour. If they are contacted by someone else or staff ask them to use a different app to chat, please report this to any member of the Safeguarding Team.
8. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
9. Parents are kindly asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
10. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
11. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
12. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.
13. Research tells us that the majority of children are now accessing artificial intelligence in some form, which is available for free on most mainstream apps and social media platforms. There are some significant risks involved with this including talking to chatbots, and the use of nudifying apps and image creators to create inappropriate and illegal images/videos I will talk to my child about these risks.
14. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
15. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
16. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games. Find out more at parentsafe.lgfl.net
17. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content. I can also set up SafeSearch to filter explicit content from searches.

18. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
19. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
20. I can find out more about online safety at St. Theresa's by reading the full Online Safety Policy here (https://www.st-theresas.barnet.sch.uk/school/policies/) and can talk to my child's class teacher, or any member of staff if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

Please note that parents may also be interested in the school's approach to the online safety, which are all covered as sections within the overall school Online Safety Policy.
~~~~~~~~~~~~~~~~~~~~~~

Appendix V: Staff, Governors and Volunteers Acceptable Use Policy

Background

We ask everyone involved in the life of St. Theresa's to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

If you have any questions about this AUP or our approach to online safety, please speak to Barbara Costa (Executive Headteacher email: office@stheresas.barnetmail.net).

What am I agreeing to?

1. **(This point for staff and governors):**
   I have read and understood St. Theresa's' full Online Safety policy (https://www.st-theresas.barnet.sch.uk/school/policies/) and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult) and make them aware of new trends and patterns that I might identify.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)
5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!
7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

8. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
10. I will check with a member of the Senior Leadership Team if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured. This includes any generative AI apps.
11. I will follow best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods.
12. I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about overblocking to the DSL.
13. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
14. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
15. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
16. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
17. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
18. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
19. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy (https://www.st-theresas.barnet.sch.uk/school/policies/). I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.
20. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.

21. I agree to adhere to all provisions of the school's Data Protection Policy (https://www.st-theresas.barnet.sch.uk/school/policies/) at all times, whether or not I am on site or using a school device, platform or network.
22. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
23. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
24. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
25. I understand that breach of this AUP and/or of the school's full Online Safety Policy here (https://www.st-theresas.barnet.sch.uk/school/policies/) may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
26. I will only use AI platforms that have been authorised for use (including those used with pupils and to support administrative tasks), and I will ensure that any use of these platforms is transparent, responsible, appropriate, legal and ethical. I will ensure that I abide by all data protection legislation in relation to using these platforms.
27. I will have a pin code on my phone.
28. I will use GDPR recommended compliant passwords.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by Barbara Costa (Executive Headteacher)

I approve this user to be allocated credentials for school systems as relevant to their role.

Additional permissions (e.g. admin) _____

Signature: _____

Name: _____

Role: _____

Date: _____