Holy Trinity CE Junior School

Policy for:	**Online Safety Policy**
Written by:	**LGfL/ Mrs Robins**
Date Adopted:	**Autumn 2024**
Review Date:	**Autumn 2026**

Holy Trinity Online-Safety Policy

Motto	**Only with Thee, O God, we journey safely on**
Vision	Exemplary education for all, through God's amazing grace.
4 year Vision target:	By the end of July 2027**: attainment and progress will remain above or within the national average; children will retain their knowledge securely; children will confidently articulate Christian values, children will be proactive learners and have aspirations for what they can achieve in life; children recognise how to behave towards one another in everyone's best interests; children will know how to be healthy, safe and enjoy life to the full!**
Values	**Learning, Dignity, Integrity, Confidence, Love**
Values statement	**Learning together, as we journey with God in Love, we act with Integrity, treat others with Dignity and grow in Confidence.**
We Learn:	**"Everything was created through Jesus and for him" Colossians 1.16.** The sub values are: Curiosity, Wisdom, Teamwork, Hard Work and Failing Well
We Love:	**"We love each other because he loved us first" 1 John 4.19.** The sub values are: Community, being Non-judgmental, Forgiveness, Compassion and Kindness
We act with Integrity:	**"People judge by outward appearance, but the Lord looks at the heart" 1 Samuel 16.7.** The sub values are: Faithfulness, Generosity, Honesty, Trustworthiness, Self-Control and Responsibility
Each person has Dignity:	**Each person has Dignity: "So God created human beings in his own image." Genesis 1.27.** The sub values are: Equality, The Whole Person, Every Person, Tolerance and Advocacy
We have Confidence:	**We have Confidence: "Blessed are those who trust in the Lord and have made the Lord their hope and confidence." Jeremiah 17:7.** The sub values are: Wholeheartedness, Hopefulness, Joy, Humility and Resilience

Holy Trinity Online-Safety Policy

Contents

Overview

Aims

This policy aims to:

- Set out expectations for all of Holy Trinity's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help 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, and regardless of device or platform
- Facilitate the safe, responsible and respectful 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
- Help 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
- Establish 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

The DSL will handle referrals to local authority multi-agency safeguarding hubs and normally the headteacher will handle referrals to the LA designated officer (LADO).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud.

Scope

This policy applies to all members of Holy Trinity community (including teaching and support staff, supply teachers and (if applicable) tutors engaged under the DfE National Tutoring Programme, admin staff, site supervisor, 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 following subjects have the clearest online safety links:

- Relationships education (RHE) and health
- Computing

However, 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/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils). We communicate with parents and carers about how we support pupils with their online safety learning

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding

School procedures for dealing with online-safety will be mostly detailed in the following policies

- Safeguarding policy and Child Protection procedures
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Mobile phone policy
- Code of conduct
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on 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 on the same day

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

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, NCA CEOP, Prevent Officer, Police, IWF). 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 disturbing or breaks the law (particular procedures are in place for sexting and upskirting).

Actions where there are concerns about a child

If staff have concerns about a child, they must pass on the information to the DSL or DDSL and record their concerns on myconcern.

Possible online safety concerns:

Sexting (Nudes- sharing nudes and semi- nudes)

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **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.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and 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.

The school DSL will 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 and next steps regarding liaising with parents and supporting pupils.

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, as highlighted in Keeping Children Safe in Education and that 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 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.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, 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

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. This includes concerns around 'deep fakes' or inappropriate use of AI. Staff should work to foster a zero-tolerance culture. 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.

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** and Mobile Phone Policy

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/handbook.

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

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the relevant policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (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 (e.g. parent or visitor), Holy Trinity 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 data security

GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply.

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements. Further, this school makes use of GDPR solution from LGfL:

GDPR.co.uk from Wonde

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

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. Egress should be used to encrypt all non-internal emails if sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times. We carry out termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy.

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools, including filters to protect against radicalisation and extremism (PREVENT).

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Holy Trinity we have decided that **option 1** is appropriate monitoring, as the filter system keeps risks to children low. Children are always supervised when online so immediate help can be offered if they see or access something they are not comfortable with; all conversations can be used as a teaching opportunity.

Google classroom is a platform which will be used for communication, should this be needed. LGfL have filters on to ensure that the platform is safe and used as staff want it to be and school admin have the ability to change settings if required.

Email

- Staff at this school use the StaffMail LGfL system for all school emails

This is linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and parents (in both directions). Use of a different platform must be approved in advance by the headteacher in advance. 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 Headteacher (if by a staff member).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately
- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, Egress systems will be deployed.
    - Internally, staff should use the school network, including when working from home when remote access is available via the Freedom2Roam system. Google drive is another platform to share and store work.
- 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
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but 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.

School website

The site is managed by Creative Schools / hosted by LGfL.

The DfE has determined information which must be available on a school website and the headteacher ensures school is complicit in this matter.

Where other staff submit information for the website, they are asked to remember:

- School 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. Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, photographs that include pupils will be selected carefully and will only feature pupils with parental permission. School newsletters are published weekly on the school website, but full names are never published alongside photographs of the relevant children. Full names of children are only published with parental permission.

Cloud platforms - google classroom

The following principles apply:

- The DPO approves new cloud systems, what may or may not be stored in them and by whom.

- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

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 and use in learning (in the parent AUP)
- For the newsletter
- For use in paper-based school marketing/ promotional work
- For online prospectus or websites
- For a specific high profile image for display or publication
- To share with parents eg year 6 leavers/ production/ class photos etc

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 Holy Trinity, no member of staff will ever use their personal phone to capture photos or videos of pupils.

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.

Although the school has an official Instagram account, it is to showcase events and share news. We will not respond to general enquiries about the school through this channel.

Staff, pupils' and parents' Social Media presence

Social media (including here 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 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, but the school regularly deals with issues arising on social media with 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 (you don't need to know them – ask your child to explain it to you), 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 is the official electronic communication channel between parents and the school, and between staff and pupils.

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). 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 of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

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 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.

Device usage

Personal devices

- **Pupils/students**: Year 5 and 6 are allowed to bring mobile phones to school, with permission from home. On arrival to school, the phone must be switched off. It is stored by the teacher and given back at the end of the day. Children should not switch the phone on again until they have left the school premises.
- **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. Phones should not be used in PPA and staff meetings. Child/staff data should never be downloaded onto a private phone. If staff need to answer an important phone call during school time, they must seek permission from the head teacher. (If a staff member needs to leave the room for an emergency call, they should ensure that their class has suitable cover, by sending a child to get another member of staff. No class can be left unsupervised; ask the caller to hold the line while supervision for the children is secured).
- **Volunteers, contractors, governors** should leave their phones in their pockets/ bags and turned off or on silent. 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 headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents:** refer to AUP

Network / internet access on school devices

- **Pupils/students** May access the internet on the wifi on a school device.
- **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. They have permission to use the school wifi. They can remote access the network on devices out of school and access the network in school.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices. (governors may have access to the wifi if the head teacher permits this.)
- **Parents** have no access to the school network or wireless internet.

Trips / events away from school

Teachers using their personal phone in to communicate will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher 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.

ANNEX A- roles and responsibilities

School staff – note that you may need to read two sections – if your role is reflected here, you should still read the "All Staff" section.

Roles:

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

Head teacher: Mrs S Gruffydd

Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- 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
- 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 GDPR-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

- 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 cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- 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 governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead: Mrs S Robins

Key responsibilities

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"
- Work with the HT and technical staff to review protections for **pupils in the home** [e.g.LGfL HomeProtect filtering for the home] and **remote-learning** procedures, rules and safeguards
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.
- 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. RHE), 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 "An effective approach to online safety [that] empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns

- 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 with the headteacher, SBM and governors to ensure a GDPR-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 RHE guidance
- Promote an awareness of and commitment to online safety throughout the school community
- Communicate regularly with SLT and the designated safeguarding and online safety governor 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. *(Staff should log on Myconcern making it clear it is on online incident.)*
- Ensure adequate provision for staff to flag issues when not in school and for pupils/ parents to disclose issues when off site, especially when in isolation/quarantine/lockdown (Myconcern)
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware
- 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).
- Facilitate training and advice for all staff, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children Annex B
    - cascade knowledge of risks and opportunities throughout the school
- 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
- Pay particular attention to **online tutors**, hired by parents.

Governing Body, led by Online Safety / Safeguarding Link Governor

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
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Ask about how the school has reviewed protections for pupils in the home (including when with online tutors) and remote-learning procedures, rules and safeguards
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- 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 co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with DSL and headteacher to ensure a GDPR-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
- "Ensure appropriate filters and appropriate monitoring systems are in place. Be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.

All staff

Key responsibilities:

- pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies
- Recognise that **RHE** is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up

- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) is- Suzanne Robins
- **Read Part 1, Annex A and Annex D of Keeping Children Safe in Education**
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident (using Myconcern)
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RHE 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)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the **20 Safeguarding Principles for Remote Lessons** infographic which applies to all online learning
- 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 GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues

Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

RHE Lead: Miss J Clark

Key responsibilities:

- As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the 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."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within RHE and ensure the policy is on the website.
- Work closely with the Computing lead 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: Miss S Alexander

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 RHE 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

Network Manager/technician – Cygnet

Key responsibilities:

- Support the HT and DSL team as they review protections for **remote-learning** procedures, rules and safeguards.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- 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

- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- 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 and cyber security policy are up to date, easy to follow and practicable

Data Protection Officer (DPO) – Judicium consulting Ltd GDPR lead: Admin

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools'
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Follow and ensure implementation of training and advice for relevant staff based on advice from our ICO, Judicium
- 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 / online safety coordinator as named in the AUP
- 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 and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor (report to CEOP if necessary)
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Support the school in promoting online safety and data protection.
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible 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.

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

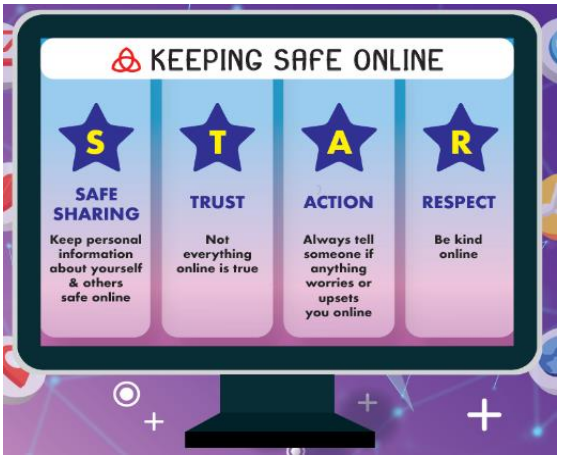
Appendices

1. *Acceptable Use Policies (AUPs) for:
    - *Pupils
    - *Staff, Volunteers Governors & Contractors
    - *Parents

We ask all children, young people and adults involved in the life of Holy Trinity 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).

Appendix 1:

Children's Acceptable Use Policy



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

All of the statements below are covered in the computing or RHE curriculum and will be referenced in the appropriate lessons across key stage 2 and in assemblies.

S- SAFE SHARING

- I understand that the school will monitor my use of the systems, devices and digital communications including if I work remotely from home.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I understand that some websites and social networks have age restrictions and I should respect this.
- I don't do live videos (livestreams) on my own –I check with a trusted adult before I video chat with anybody for the first time.
- 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 won't share or say anything that 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.
- I know that the filter system is in place to keep me safe. If a site does get through the filter system that is inappropriate I will tell an adult immediately and won't share it with anyone.
- I know I leave a digital footprint and I know anything I do can be shared and might stay online forever

T- TRUST

- I won't meet up in real life with online friend. If I want to do so I will discuss this with a trusted adult. IF I am allowed, I will never go alone.

- I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

A- ACTION

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that if someone sends me something bad I won't be in trouble but I mustn't share it. Instead I should tell an adult.
- I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

R- Respect

- I will not post, make or share unkind hurtful or rude messages/ comments. If I see this happening I will tell an adult.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I should ensure that I have permission to use the original work of others in my own work.
- I know just calling something banter doesn't make it ok as it could become bullying. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may lose access to the school internet and remote access. My parents will be contacted and the behaviour policy will be adhered to. In the event of illegal activities involvement, the police may be involved.

Appendix 2

Staff, Volunteers and Governors: Acceptable Use Policy

What am I agreeing to?

1. I have read and understood full Online Safety policy 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.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead- Mrs Robins (if by a child) or Head teacher- Mrs Gruffydd (if by an adult).
3. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the RHE curriculum, as well as safeguarding considerations if supporting pupils remotely.
4. I will take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment - and maintain an attitude of 'it could happen here'
5. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
6. Emails that I send will be professional in content and in line with the school's values.
7. 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 if concerns are raised that deem this necessary. (HT for any concerns raised regrading professional conduct and DSL if concerns raised regarding child safeguarding.)
8. 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, including social media.
9. 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. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
10. 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 not sure if I am allowed to do something in or related to school, **I will not do it.**

    I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home. I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
11. I understand the importance of upholding my online reputation, my professional reputation (and that of the school), and I will do nothing to impair either.

12. I will use the school Whatsapp group (that is linked to business continuity plan) **professionally** at all times. I will not use children's full names in any Whatsapp communication.
13. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify Mrs Eden if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
14. 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.
15. 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 by the school.
16. 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.
17. I will report any concerns with the Head teacher or Chair of governors if I believe that staff are not adhering to this AUP.
18. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents. I have read the sections in the policy on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
19. **If there are any periods of remote learning:**
    - **I will not behave any differently** towards students compared to when I am in school. I 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.
    - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
    - **I will not take secret recordings or screenshots** of myself or pupils during live lessons.
    - **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
    - **I will inform SLT following live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students.
    - **I will record any google meets that I am asked to** I know the recordings will be kept for a set time in the cloud before being deleted.
    - **If I need to contact a parent whilst working from home, I will block my number.**
20. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Name:_____ Date:_____

Signature:_____

Appendix 3:

Parents Acceptable use policy

What am I agreeing to?

1. I understand that Holy Trinity 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 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 behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and devices used in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, including during any remote learning periods.
4. 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.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using the various platforms of social media. I will support the school and not encourage my child to join any platform where they are below the minimum age (including but not exclusively- Whatsapp (13+), Snapchat (13+), Facebook (13+), Instagram (13+), TikTok (13+))
6. I will not share images of other people's children (including video images) on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. I will not use any 'live streaming' to record images within the school. I know that 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.
7. 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 know I can refer to parentsafe.lgfl.net for advice and support on safe settings.
8. I understand that my child needs a safe and appropriate place to do remote learning if school are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, 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.

9. I understand that if my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster. I know to 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.
10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and can contact my internet provider if I need support. I will monitor my child when they access the internet.
11. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child/ren.
12. 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.
13. I can find out more about online safety by reading the full Online Safety Policy on the website and can talk to my child's class teacher or SLT 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.
14. I know that if my child has received any malicious communications I can call 101. I know that if I have serious concerns about my child's online safety I can report this to **Child Exploitation and Online Protection (CEOP)**

As the parent or legal guardian of the pupil(s) named below I grant permission for the school to take photos of my child to use within the building.(eg: displays around the school to celebrate success such as; photos to display school council; photos of children at work to be printed and stuck into their work books.)

In the case a situation that requires remote learning: As the parent or legal guardian of the pupil(s) named below I grant permission for my child to attend a scheduled 'google meet' as an online video conference. I understand the sessions may be recorded for safeguarding reasons.

15. During any remote learning periods, I understand that my child might be contacted online by the class teacher or year group support staff (in cases of remote learning) via google classroom and only about their learning, wellbeing or behaviour. If they are contacted by someone else or these staff ask them to use a different app to chat, they will tell another teacher

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

My daughter / son name(s): _____

Parent / guardian signature: _____ Date: ___/___/___