Liverpool
City Council

St Cleopas C of E Primary School

Mission Statement: We are a distinctive, inclusive, Christian school, where everyone is welcomed and valued. We aim to nurture and develop opportunities for lifelong learning through a caring and inclusive ethos. We seek to help children to know God and find ways of relating to Him. We come together in a friendly, creative community to develop our cultural lives, spirituality and abilities through the core values of Love, Trust, Care, Respect and Joy all given and received in Jesus' name.

Biblical Reference:

"..love one another. As I have loved you, so you must love one another, then everyone will know that you are my disciples".

John 13:34-35

1. Introduction – key people/dates

This Online Safety policy has been developed and reviewed (April 2023) by a working group made up of:

- School Safeguarding Leader (Mr I Fitzgerald)
- School Computing Lead (Miss N Kavanagh)
- Headteacher / Senior Leaders
- Teachers
- Support Staff
- Governors

The implementation of this online safety policy will be monitored by the:	• Safeguarding Lead: Mr I Fitzgerald • Safeguarding Team: Mrs L Gannon, Mr J Conn, Mrs A Berry • Safeguarding Governor: Mrs K Morris • Governors
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	• April 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	• See page 8, 9 & 10 of this document

i. Purpose of this policy

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Provide staff, pupils and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

This policy should be read alongside Part 1 and Annex B of Keeping Children Safe in Education 2022, and in conjunction with Section 1 of the School Improvement Liverpool Schools Safeguarding Handbook which is made available to all staff and volunteers.

ii. Who is this policy for?

This policy statement applies to **all** staff, visitors, volunteers, children and anyone involved in St Cleopas' Church of England Primary School activities. This policy provides guidance to all adults working within the school whether paid or voluntary or directly employed by the school or by a third party.

iii. Who is in charge of online safety?

Online safety requires a whole-school approach. Whole school approaches are likely to make teaching more effective than lessons alone. A whole school approach is one that goes beyond teaching to include all aspects of school life, including: culture, ethos, environment and partnerships with families and the community.[1]

According to the *Keeping Children Safe in Education* (2022), "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." [2]Whilst the Designated Safeguarding Lead will take lead responsibility of safeguarding, all children, staff and any other volunteer involved in the community of St Cleopas Church of England Primary School are required to play a role in safe internet usage. The school computing lead and PSHE lead will also plan and coordinate activities alongside the teaching staff to ensure children cover appropriate online safety modules suited to the current risks presented by technology.

iv. How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for <u>all</u> new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school staff room.

v. What are the main online safety risks in 2023/2024?

We live in a digital age where technology is playing an ever-increasing part in our lives; it is changing the way that we do things both inside and outside of school. Although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

St Cleopas Church of England Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material.

- Contact: being subjected to harmful online interaction with other users.

[1] Department for Education, Guidance: Teaching Online Safety in School, 12 January 2023, https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools&whole-school-approach

[2] Department for Education, Keeping Children Safe in Education, September 2022, p.28, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

- Conduct: personal online behaviour that increases the likelihood of harm
- Commerce: being subjected to risks such as gambling and financial scams.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks, it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Contents

2. Overview

i. Aims

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

- Setting out expectations for all St Cleopas' Church of England Primary 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 filtering and monitoring through effective collaboration and communication with technical colleagues
- 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)

ii. Scope

As previously stated, this policy applies to all members of the St Cleopas Church of England Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, 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.

3. 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.

Depending on their role, all members of the school community should read the relevant section in Annex A of this document that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex (insert hyperlink)

4. Education and Curriculum

Online Safety will be taught throughout a relevant and progressive curriculum in both computing and PSHE lessons using a range of teaching materials, including the Purple Mash online safety resources, Jigsaw and the National Curriculum 2014.

We will ensure that:

- All children, parents and staff complete an internet acceptable user agreement which sets out rules for internet use while in school.
- Parents are kept up to date with relevant online safety information through our home/school Twitter and website page.
- Data policies stipulate how we keep confidential information secure.
- Training opportunities are provided for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- Filtering and monitoring systems are in place for all of our online access.
- All school owned devices will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledges the source of information.
- Supervision of pupils will be appropriate to their age and ability.
- All internet use must be for educational purposes

The curriculum is carefully planned to teach about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app. This 'rolling' curriculum is reviewed on a yearly basis reviewed to support the specific needs of pupils, including vulnerable pupils.

The curriculum is reviewed regularly based on monitoring of the PSHE and computing curriculum in addition to feedback from pupil voice and staff.

For further information on the progression in the digital literacy aspect of computing at St Cleopas view: Computing Progression Map

Through use of Purple Mash, each year group will have the opportunity to engage in one Online Safety module per year: Computing Long Term Plan. This is reviewed annually to ensure this coverage is relevant to current issues in the evolving digital age.

Issues such as cyberbullying and staying safe online are also addressed during PSHE lessons (PSHE/RSE Curriculum), Collective Worship sessions, Anti-bullying Week, Safer Internet Day and any other opportunities seen fit by the class teacher. 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)

5. Inclusion

St Cleopas Church of England Primary School recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. St Cleopas will ensure that adaptive and ability appropriate online safety education, access and support is provided to vulnerable pupils. When implementing an appropriate online safety policy and curriculum, we seek input from specialist staff as appropriate, including the SENDCO and Designated Safeguarding Leads. The computing lead will keep up-to-date with any developments regarding emerging technologies and online safety and how these may impact on pupils with special educational needs.

6. Remote Learning

In the event of school closures, St Cleopas will often utilise online learning as a platform to continue education. The main platform used will be Purple Mash. Any online learning tools or systems recommended for use by St Cleopas, are be in line with privacy and data protection/GDPR requirements. Pupils have access to Purple Mash at home with their own individual logins and passwords.

St Cleopas' encourage parents and carers to **closely monitor** children's usage to ensure they are accessing the relevant tasks and avoiding any other sites which may have risks such as those detailed on page 4 of this document.

For further advice on how you can support your child at home, refer to page 30 of this document.

Where children are not physically attending a Hub/school, St Cleopas will consider the safety of our children when they are asked to work online. The starting point for online teaching remains the same as the principles set out in our school's staff code of conduct. This policy includes acceptable use of technologies, staff/pupil relationships and communication including the use of social media. This policy applies equally to any existing or new online and distance learning arrangements which have been introduced.

Families will be made aware of what their children are being asked to do online, including the sites they will be asked to access and who their child is going to be interacting with online, including members of staff from our school. We will signpost parents to support using our school's website and Twitter page.

7. Handling online-safety concerns and incidents

All St Cleopas staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RSE. General concerns must be handled in the same way as any other safeguarding concern, reporting to the DSL in a prompt manner.

St Cleopas 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 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.

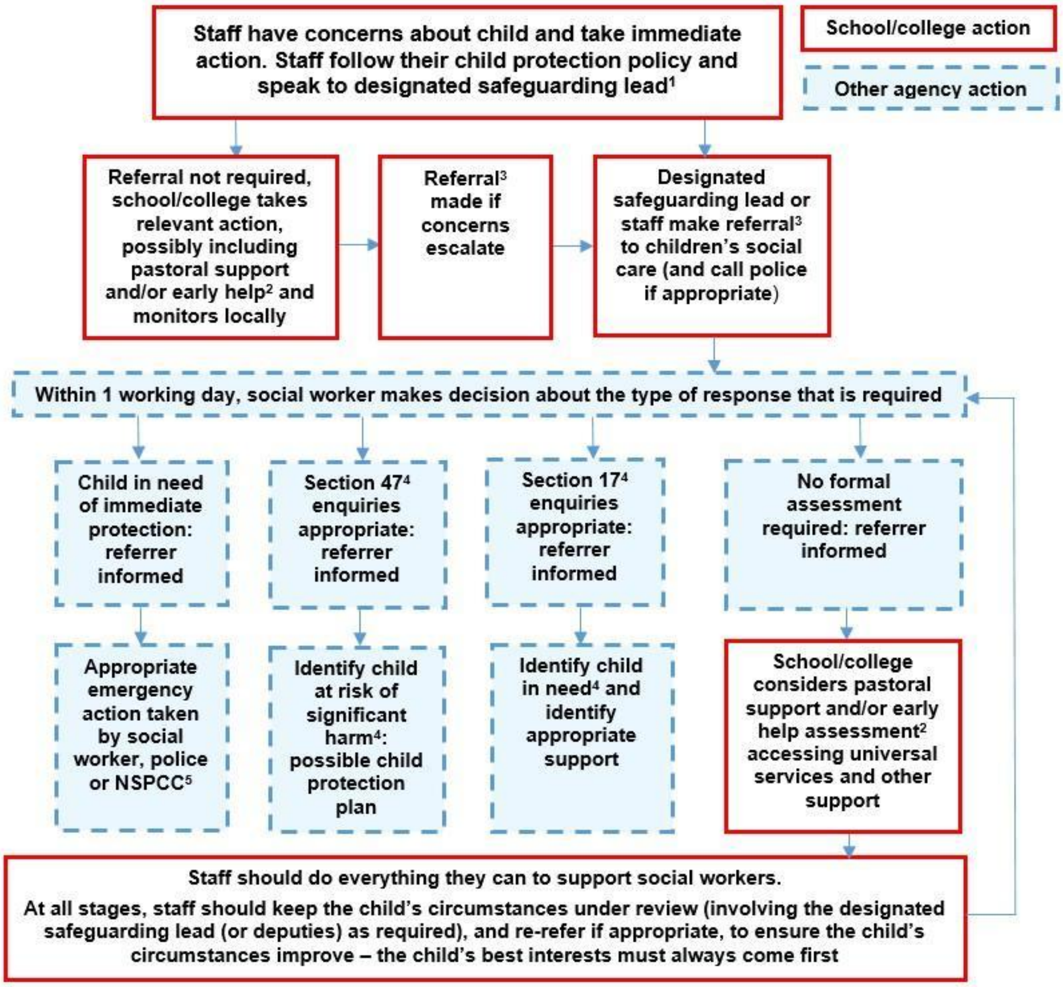
Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed.

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; see section below).

i. Actions where there is a concern about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 [3]as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead1
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help2 and monitors locally
Referral3 made if concerns escalate
Designated safeguarding lead or staff make referral3 to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 474 enquiries appropriate: referrer informed
Section 174 enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC5
Identify child at risk of significant harm4: possible child protection plan
Identify child in need4 and identify appropriate support
School/college considers pastoral support and/or early help assessment2 accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

[If you have ANY concerns about a child's welfare or well-being or have a concern about the behaviour of any adult within the school towards a child:

- Discuss your concerns without delay with the Designated Safeguarding Lead or the Headteacher or a member of the safeguarding team.
- Remember it is important to share your concerns even if you are unsure.
- Anyone can make a referral to Liverpool Children's Services (tel: 0151 233 3700)
- The Local Authority Designated Officer (L.A.D.O.) for Managing Allegations Against Staff can be contacted on 0151 225 8101. The school office can provide you with a copy of the school's 's procedures for Managing Allegations Against Staff.

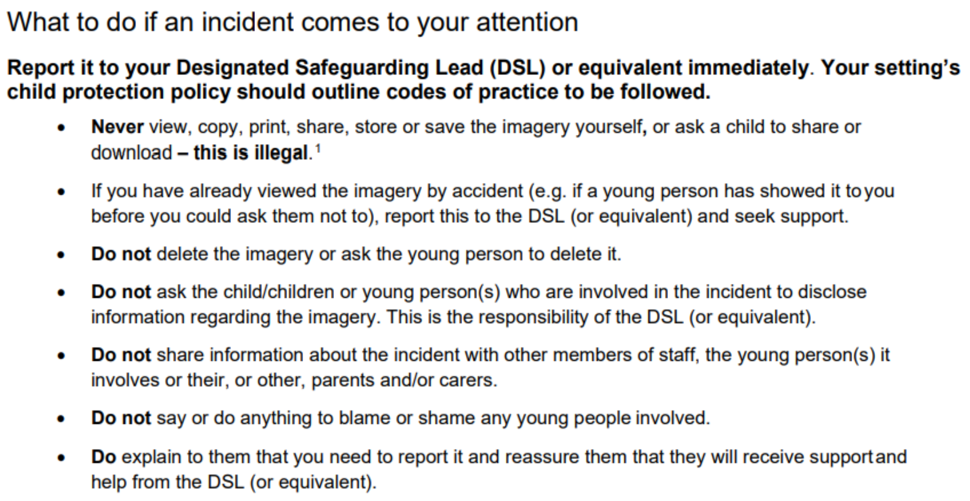
Designated Safeguarding Lead	Mr I Fitzgerald
Deputy Safeguarding Lead	Mrs L Gannon
Safeguarding Team	Mr J Conn, Mrs A Berry
Safeguarding Governor	Mrs K Morris

[3] Department for Education – Keeping Children Safe in Education, September 2022, p.22, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

ii. Sharing nudes and semi-nudes / sexting

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings][4] to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

All staff (not just classroom-based staff) are required to read and follow the advice in the document as 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.

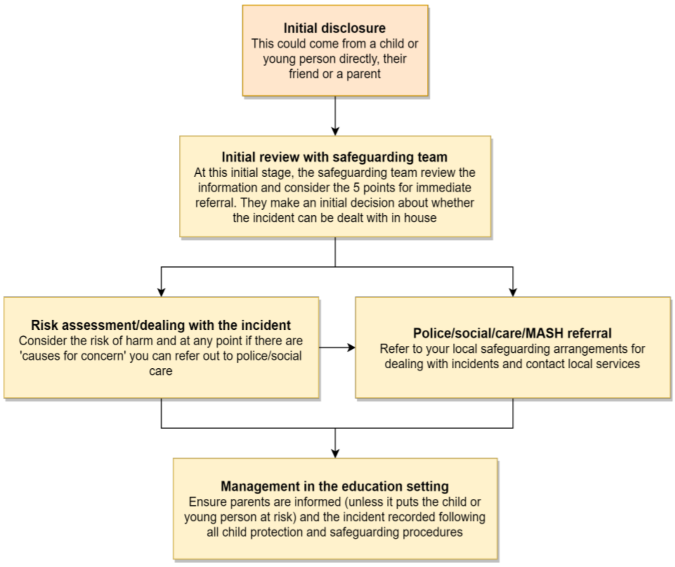


What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. Your setting's child protection policy should outline codes of practice to be followed.

- **Never** view, copy, print, share, store or save the imagery yourself**,** or ask a child to share or download **– this is illegal.**[1]
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

When dealing with an incident, 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.


Initial disclosure
This could come from a child or young person directly, their friend or a parent
Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house
Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care
Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services
Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

***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

Whilst sexting is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

[4] UKCIS guidance: *Sharing Nudes and semi-nudes: advice for education settings working with children and young people* (23 December 2020): https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

iii. Online Bullying

St Cleopas takes on a zero-tolerance approach to any aspects of bullying. This applies to online bullying, which is considered peer on peer abuse in the Keeping Child Safe in Education document. Where we receive a report of peer on peer abuse, we will follow the principles as set out in part 5 of KCSIE and of those outlined within our main Child Protection policy. We will listen and work with the young person, parents/carers and any multi-agency partner required to ensure the safety and security of that young person. Concerns and actions will be recorded using the agreed methods and appropriate referrals made as per the school's safeguarding policy. For information on how to report any safeguarding concern, please refer to page 9 & 10 of this document.

Our school encourages parents and carers to closely monitor their child's online usage at home and ensure that relevant filtering systems, such as parental locks, are in place to protect their children. Please refer to page 26 & 27 for more guidance on how to protect your child.

iv. 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 Cleopas community. These are also governed by school Acceptable Use Policies and the school social media 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, St Cleopas 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.

8. Data Protection and Data Security

Please refer to St Cleopas' Data Protection Policy for guidance on Data Protection, Data Storage and all other GDPR related information. All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found here: St Cleopas' Data Protection Policy[5] and St Cleopas' GDPR Privacy Notice[6]

The headteacher/principal, 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.

9. Filtering, Monitoring and Reporting

The school's broadband is provided by an external company named RM. As part of that, filtering is carried out from RM Safety Net which aims to block access to any inappropriate sites which fit the criteria on page 3 & 4 of this document. This system is regularly viewed and updated by an external company, Liverpool IT Services, with the most

[5] St Cleopas' *Data Protection Policy* (2021): https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Data-Protection-2.pdf

[6] St Cleopas' GDPR Privacy Notice (2021) : https://www.stcleopas.co.uk/wp-content/uploads/2021/06/privacy-notice.pdf

recent sites. In addition to the security and filtering process, RM Safety Net can be customised by Senior Leadership with access to block any new sites, such as: gaming sites which may have a chat box setting.

The RM Safety Net has notifications in place which flag up to Senior Leadership Team as an automatic email with any safeguarding concerns. The governors are kept up to date with a list of filtering and monitoring reports through the safeguarding agenda at governor's meetings.

Relevant training and development will be delivered when necessary by the Safeguarding Team. Times this will be necessary include: when legislation changes or there is new guidance from the government. St Cleopas' Church of England Primary School consider online safety a major priority when training staff, governors and visitors to our school.

10. Use of technology within lessons

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

i. Early Years Foundation Stage

Within Nursery and Reception at St Cleopas, we encourage parent partnership through the use of Tapestry, an online learning journal which parents can access at home. [7]

Due to curriculum changes, children in EYFS don't access to the internet during lesson times. While children do not access the internet at school, safety is discussed within their Early Learning Goals, in addition to opportunities developed by staff and adapted to suit the needs of cohorts.

ii. Key Stage 1

The aims of the National Curriculum require all children to become responsible, competent, confident and creative users of information and communication technology

As part of the DFE's National Curriculum for computing, children in Key Stage 1 are required to:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies[8]

iii. Key Stage 2

The aims of the National Curriculum require all children to become responsible, competent, confident and creative users of information and communication technology

As part of the DFE's National Curriculum for computing, children in Key Stage 2 are required to:

[7] St Cleopas' Early Years Foundation Stage Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/12/EYFS-Policy-A.pdf

[8] Department for Education, Statutory guidance - National curriculum in England: computing programmes of study, 11 September 2013: https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study

- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.[9]

All of the above are embedded throughout St Cleopas' computing curriculum.

11. Training and Development

As per the Keeping Children safe in education document, staff will receive appropriate safeguarding and child protection training (including online safety) at induction. The training will be regularly updated. In addition, all staff will receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.[10]

As per regular meetings, governing bodies will ensure that all staff undergo safeguarding and child protection training[11] (including online safety) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners.

As part of St Cleopas' whole school approach, the children are taught about online safety by their teachers through a carefully planned and reviewed curriculum.

12. 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. Members of staff may take photographs of children whilst engaged in school activities for teaching purposes.

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: St Cleopas' Data Protection Policy

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 Cleopas, 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, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

[9] Department for Education, Statutory guidance - National curriculum in England: computing programmes of study, 11 September 2013: https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study

[10] DFE, *Keeping Children Safe in Education*, (2022), p.8, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

[11] DFE, *Keeping Children Safe in Education*, (2022), p.32, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

While the school will discourage the use of photography from parents and members of the public at school functions, the school cannot however be held accountable for photographs or video footage taken by parents or members of the public.

13. Social Media

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), however it is worth nothing that incidents regarding these platforms are becoming increasingly common across many primary schools.

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). *Refer to page 26 of this document for further advice.*

The school has an official Twitter account (managed by SLT) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

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[12].

14. Device Usage

All staff, pupils, parents, governors and visitors are required to adhere to the Acceptable Usage Policies. For further information regarding mobile phones, refer to the St Cleopas' Mobile Phone Policy available at this link: St Cleopas' Mobile Phone Policy

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 acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

15. 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.

Full details of the school's search procedures are available in the school Behaviour Policy: St Cleopas' Behaviour Policy

[12] St Cleopas' *Data Protection Policy* (2021): https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Data-Protection-2.pdf

If the correct code of conduct is not followed with any electronic device on site, the headteacher reserves the right to request these devices back and report the unsafe use to the relevant bodies. [13] *To report unsafe usage, please refer to the document on page 9 & 10.*

Complaints about screening or searching should be dealt with through the normal school complaints procedure available via the school website.

[13] Department for Education: *Searching, screening and confiscation* (2018), pp.13 - 14: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091133/Searching_screening_and_confiscation_advice_2014__updated_2018_.pdf

Appendix 1

Role and responsibilities

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

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 (Mrs L Gannon)
- Designated Safeguarding Lead (Mr I Fitzgerald)
- Governing Body, led by Safeguarding Link Governor (Mrs K Morris)
- PSHE / RSHE Lead (Ms K McDowell)
- Computing Lead (Ms N Kavanagh)
- Subject leaders
- Network Manager/technician
- Governors, volunteers and contractors (including all visitors)
- Pupils
- Parents/carers

All Staff

Key Responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know who the Designated Safeguarding Lead (DSL) is [Mr I Fitzgerald]; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Sign and follow the staff acceptable use policy and code of conduct/handbook.
- 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)
- 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.
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting pupils remotely, be mindful of additional safeguarding considerations.
- 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 sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils/students 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 all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know.
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues.
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside 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.

Headteacher – Mrs L Gannon

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 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
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how. Note that KCSIE 2022 strengthens the wording for this.
- 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.
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process (this new addition has come into KCSIE 2022 for the first time)
- 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
- 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 – Mr I Fitzgerald

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** and **remote-learning** procedures, rules and safeguards.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective whole school approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
- Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees 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 online safety 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 headteacher, DPO 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/trustees.
- 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 RSHE 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, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety 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/lockdown, e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why. Also, as per KCSIE "be careful that 'over blocking' does not lead to unreasonable restrictions."
- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that 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.

Governing Body led by Safeguarding Link Governor – Mrs K Morris

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

- Approve this policy and strategy and subsequently review its effectiveness.
- Undergo (and signpost all other governors and Trustees 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
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- 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 coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, 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
- 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) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach."
- "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.

Computing Lead

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 RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL 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
- Carry out pupil voice each term to review pupils' understanding of online safety and relay this information to DSL and staff so that the curriculum can be amended appropriately.

PSHE Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe 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."
- This complements 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 and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE 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

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 new 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/ Technician

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. Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.
- 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.
- 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 / RSHE 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.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Governors/Volunteers/ Contractors/Visitors

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

- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- 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
- 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

Parent/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.
- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and 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.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available on page

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 2a

Related Policy and Documents

Please refer to the below documents for further information regarding online safety at St Cleopas Church of England Primary School.

1. St Cleopas' Safeguarding Incident Log and Reporting System (via Mr I Fitzgerald)
2. Safeguarding Policy: https://www.stcleopas.co.uk/wp-content/uploads/2022/11/Safeguarding-policy-2022-23.pdf
3. Child Protection Policy: https://www.stcleopas.co.uk/wp-content/uploads/2022/11/CP-Policy-Sept-2022.pdf
4. Behaviour Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/06/st-cleopas-behaviour-policy.pdf
5. Anti-Bullying Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Anti-Bullying-Policy-2.pdf
6. Staff Code of Conduct / Handbook
7. Acceptable Use Policies
   - Pupils
   - Staff, Governors, Volunteers & Contractors
   - Parents
8. Use of Social Media Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Use-of-Social-Media-Policy-A.pdf
9. Mobile Phone Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Mobile-Phone-Policy-A.pdf
10. Data Protection Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Data-Protection-2.pdf
11. Keeping Children Safe in Education 2022 Part 1 and Annex A https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf
12. Letters to Parents about filming/photographing/streaming school events
13. Computing Curriculum: https://www.stcleopas.co.uk/wp-content/uploads/2022/03/Computing-LTP-2021-2022.pdf
14. PSHE/RSE Curriculum: https://www.stcleopas.co.uk/wp-content/uploads/2022/09/PSHE-RSE-Curriculum.pdf
15. Early Years Foundation Policy: https://www.stcleopas.co.uk/wp-content/uploads/2021/12/EYFS-Policy-A.pdf

Appendix 2b

Further Reading and Information

This policy also takes in account advice from: https://www.gov.uk/topic/schools-colleges-childrens-services/safeguarding-children

This advice includes:

- Department for Education guidance: *Teaching online safety in schools* (2023): https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools
- UK Council for Internet Safety (UKCIS) guidance: *Education for a connected world* (2020): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf
- Department for Education: *Safeguarding children and protecting professionals in early years settings: online safety considerations* (2019): https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations
- Department for Education: *National Curriculum in England: Computing Programmes of Study* (2013): https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study
- Department for Education: *Harmful online challenges and online hoaxes* (2021): https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes
- Safer Recruitment Consortium: *Safer working practice for those working with children & young people in education* (February 2022): https://c-cluster-110.uploads.documents.cimpress.io/v1/uploads/d71d6fd8-b99e-4327-b8fd-1ac968b768a4~110/original?tenant=vbu-digital
- Department for Education: *Relationships Education, Relationships and Sex Education (RSE) and Health Education* (2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1090195/Relationships_Education_RSE_and_Health_Education.pdf
- Department for Education: *Working together to safeguard children* (2022): https://www.gov.uk/government/publications/working-together-to-safeguard-children--2
- Department for Education: *Searching, screening and confiscation* (2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091133/Searching_screening_and_confiscation_advice_2014__updated_2018_.pdf

- Department for Education*: Promoting fundamental British values as part of SMSC in schools* (2014): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/380595/SMSC_Guidance_Maintained_Schools.pdf
- UKCIS guidance: *Sharing Nudes and semi-nudes: advice for education settings working with children and young people* (2020): https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
    - How to respond to an incident – overview for all staff
    - Full guidance for schools DSLs
- Department for Education: *Prevent Duty Guidance for Schools* (2021) : https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales
- Department for Education: *Preventing Bullying & Cyber Bullying* (2017): https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- The National Grid for Learning: *RAG (red- amber-green) audits for statutory requirements of school websites* (2020): https://national.lgfl.net/digisafe/school-website-rag-audit-tool
- Ofsted: *Review of sexual abuse in schools and colleges* (2021): https://www.gov.uk/government/publications/review-of-sexual-abuse-in-schools-and-colleges/review-of-sexual-abuse-in-schools-and-colleges

Appendix 3

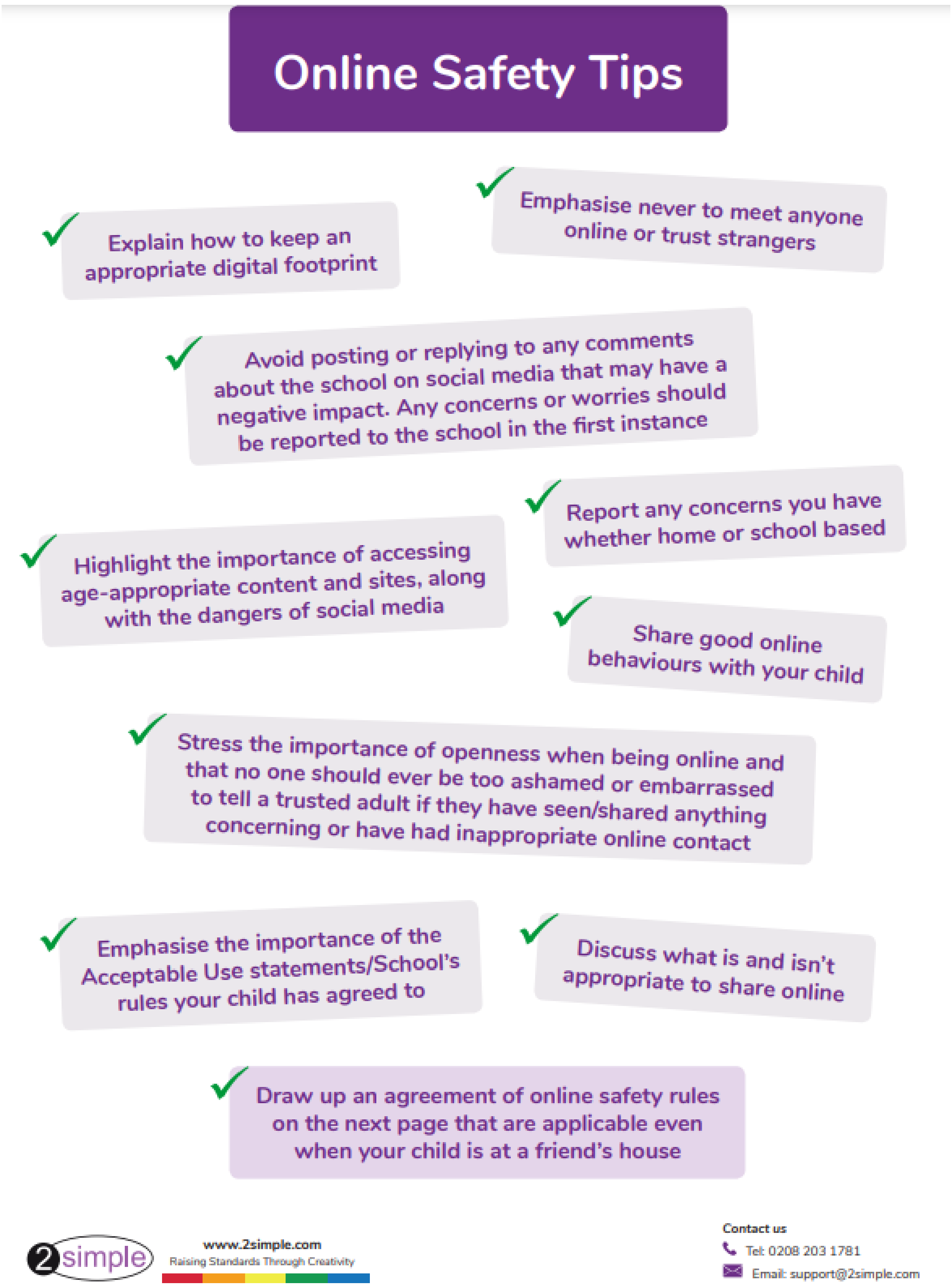
Useful Support/Guidance for Parents and Carers

Below is a complied list of resources which may support you in dealing with online safety and supporting your child in a digital age. Please note these are third party sites offered as support and guidance in dealing with issues that may arise at home. These have not been created by or are not monitored by St Cleopas Church of England Primary School.

Please refer to our safeguarding and child protection policies to report any incidents which may arise within school.

Name of site	Info	Web Address
Thinkuknow	The site offers materials for parents and pupils on a wide range of online safety issues and facts about areas such as digital footprints, recognising fake websites and checking URLs.	https://www.thinkuknow.co.uk/
Every Mind Matters	This site offers materials for parents, teachers and pupils on areas such as cyberbullying, social media, online stress and body image in a digital world.	https://campaignresources.phe.gov.uk/schools/topics/mental-wellbeing/overview
UK Safer Internet Centre	This site offers advice on laptops, phones, smart speakers, game consoles, tablets and smart TVs.	https://saferinternet.org.uk/guide-and-resource/parents-and-carers
UK Safer Internet Centre	This site offers advice on social media.	https://saferinternet.org.uk/guide-and-resource/social-media-guides
Childnet	This site offers advice on reliability online, digital wellbeing, gaming and other issues.	https://www.childnet.com/parents-and-carers/
Internet Watch Foundation	This site offers advice on online sexual abuse.	https://www.iwf.org.uk/
South West Grid for Learning (SWGfL)	This site offers online safety training for parents, carers and children.	https://swgfl.org.uk/training/online-safety-training/
NSPCC	This site offers advice on online wellbeing, parental controls and starting a conversation with your child.	https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Parent Safe	This site offers advice on safety controls and screen time.	https://parentsafe.lgfl.net/

Purple Mash Online Safety Tips for Parents/Carers



Online Safety Tips

✓ Explain how to keep an appropriate digital footprint

✓ Emphasise never to meet anyone online or trust strangers

✓ Avoid posting or replying to any comments about the school on social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance

✓ Highlight the importance of accessing age-appropriate content and sites, along with the dangers of social media

✓ Report any concerns you have whether home or school based

✓ Share good online behaviours with your child

✓ Stress the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact

✓ Emphasise the importance of the Acceptable Use statements/School's rules your child has agreed to

✓ Discuss what is and isn't appropriate to share online

✓ Draw up an agreement of online safety rules on the next page that are applicable even when your child is at a friend's house

2simple

www.2simple.com
Raising Standards Through Creativity

Contact us
☎ Tel: 0208 203 1781
✉ Email: support@2simple.com

Appendix 4a

Acceptable Use Policy for Pupils

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ✓ I will keep my username and password secure; this includes not sharing it with others.
- ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ✓ I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- ✓ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- ✓ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- ✓ Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = is it true?
  H = is it helpful?
  I = is it inspiring?
  N = is it necessary?
  K = is it kind?

- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My Name:

Class:

Date:

Appendix 4b

Acceptable Use Policy for Staff, Volunteers, Visitors and Contractors

- ✓ I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
- ✓ 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. The same applies to any private/direct communication with a pupil.
- ✓ I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students.
- ✓ If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- ✓ If I am given access to school-owned devices, networks, cloud platforms or other technology:
  - ✓ I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
  - ✓ I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role
  - ✓ I will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
  - ✓ I will protect my username/password and notify the school of any concerns
  - ✓ I will abide by the terms of the school Data Protection Policy and GDPR protections https://www.stcleopas.co.uk/wp-content/uploads/2021/11/Data-Protection-2.pdf
- ✓ I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
- ✓ I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
- ✓ I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils/students and will not give any advice on online-safety issues unless this is the purpose of my visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).
- ✓ I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead – Mr I Fitzgerald (if by a child) or Headteacher – Ms L Gannon (if by an adult).
- ✓ I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance.
- ✓ I will not view material which is or could be perceived to be inappropriate for children or an educational setting.
- ✓ If I have any questions during or after my visit, I will ask the person accompanying me (if appropriate) and/or Mr I.Fitzgerald (Designated Safeguarding Lead at St Cleopas Church of England Primary School). In the event this member is not available, I will contact the Ms L.Gannon (Headteacher and Deputy Safeguarding Lead at St Cleopas Church of England Primary School) or the next relevant safeguarding body.

To be completed by staff/visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: ______________________________

Name: ______________________________

Organisation: ______________________________

Visiting / accompanied by: ______________________________

Date / time: ______________________________

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: ______________________________

Name / role / date / time: ______________________________

Appendix 4c

Acceptable Use Policy for Parents

Background and Purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

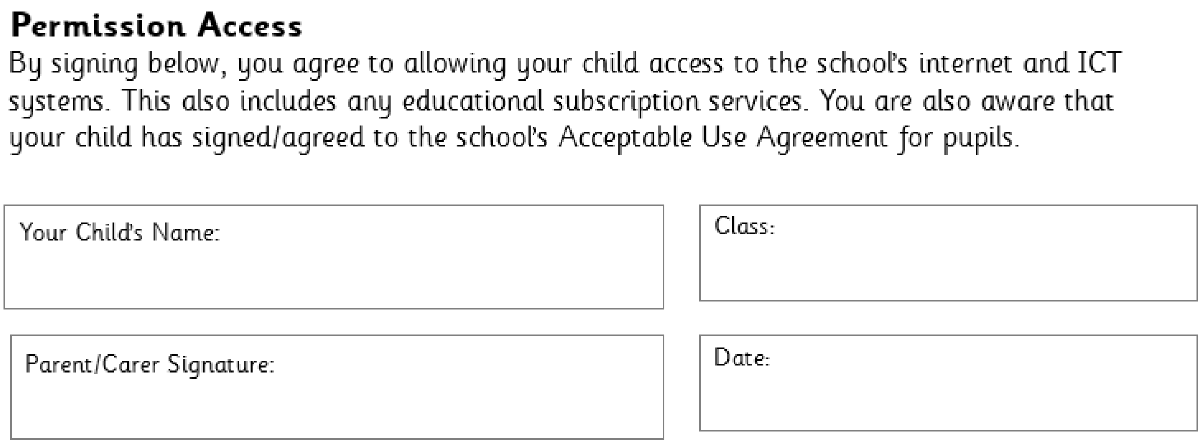
This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting.

St Cleopas will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

Parents/Carers

We ask parents and carers to support us by:

- ✓ Sharing good online behaviours with your child.
- ✓ Emphasising the importance of the Acceptable Use Statements/School's rules your child has agreed to.
- ✓ Highlighting the importance of accessing only age appropriate content and sites along with the pitfalls of social media.
- ✓ Explaining how to keep an appropriate digital footprint.
- ✓ Discussing what is and isn't appropriate to share online.
- ✓ Emphasising never to meet anyone online nor trust that everyone has good intentions.
- ✓ Reporting any concerns you have whether home or school based.
- ✓ Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- ✓ Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- ✓ Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.



Permission Access

By signing below, you agree to allowing your child access to the school's internet and ICT systems. This also includes any educational subscription services. You are also aware that your child has signed/agreed to the school's Acceptable Use Agreement for pupils.

Your Child's Name:

Class:

Parent/Carer Signature:

Date: