St Gabriel’s C of E Primary School

Online Safety Policy
AUTUMN 2025

Committee Name:	Standards and Achievement Committee
Date of Review:	October 2025
Validity Date:	October 2025-October 2026
Online-safety lead:	Sonia Bell
Online-safety / safeguarding link governor	Valerie Michelet
Data Protection Officer (DPO)	John Pearson- Hicks

1. Introduction and Overview Rationale

At St Gabriel's Primary School, we are committed to providing a safe and supportive online environment for all members of our community, including pupils, staff, volunteers, and governors. Our aims are to implement robust and effective processes that ensure the online safety and wellbeing of everyone within the school community. We strive to identify and provide targeted support for groups of pupils who may be at increased risk of online harm or vulnerability. Our approach to online safety is comprehensive and proactive, empowering the entire school community to use technology responsibly and safely, including mobile and smart devices. Additionally, we have established clear and well-defined procedures to identify, respond to, and escalate online safety incidents swiftly and appropriately.

The purpose of this policy is to:

- **Set out key principles** expected of all members of the St Gabriel's Primary School community regarding online behaviour, attitudes, and activities, including the use of digital technology both on and offline.
- **Safeguard and protect** pupils and staff from online risks and harms.
- **Support safeguarding and senior leadership teams** by enhancing understanding and awareness of filtering and monitoring systems through effective collaboration and communication with technical colleagues.
- **Reinforce that online and digital behaviour standards** (including social media activity) must be upheld beyond the school premises and school hours, regardless of device or platform.
- **Facilitate the safe, responsible, and respectful use of technology** to support teaching and learning, improve pupil attainment, and prepare pupils for the risks and opportunities of today's and tomorrow's digital world—enabling them to survive and thrive online.
- **Clarify the roles and responsibilities of school staff** working with pupils to ensure they use technology safely and responsibly:

➢ For the protection and benefit of pupils in their care.

➢ For their own protection, minimising the risk of misplaced or malicious allegations, and to ensure clarity around professional standards and practice.

➢ For the benefit of the school, supporting its ethos, aims, and objectives, and protecting the reputation of the school and the teaching profession.

- **Establish clear procedures and structures** for addressing online misdemeanours and concerns, with reference to related policies such as the Behaviour Policy and Anti-Bullying Policy.

The main areas of risk for our school community can be summarised as follows:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual

sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

• **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- **Teaching online safety in schools**
- **Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff**
- **Relationships and sex education (RSE) and health education**
- **Searching, screening and confiscation**

It also refers to the DfE’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also considers the National Curriculum computing programmes of study.

3. Role and Key Responsibilities

The governing board	The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online. The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE’s filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include: • Identifying and assigning roles and responsibilities to manage filtering and monitoring systems • Reviewing filtering and monitoring provisions at least annually • Blocking harmful and inappropriate content without unreasonably impacting teaching and learning 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) • Having effective monitoring strategies in place that meet the school's safeguarding needs • The governor who oversees online safety is **Valerie Michelet** • All governors will: • Make sure they have read and understand this policy • Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4) • Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures • Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
The Headteacher: Rebecca Anson	The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.
The Designated safeguarding lead (DSL): Rebecca Anson **The Deputy safeguarding leads:** Sonia Bell Mark Nunn	Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular: • Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school • Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly • Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks • Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly • Working with the ICT manager to make sure the appropriate systems and processes are in place • Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents • Managing all online safety issues and incidents in line with the school's child protection policy • Responding to safeguarding concerns identified by filtering and monitoring • Making sure that any online safety incidents are logged by filling in the Safeguarding/Child Protection Recording Concerns (Appendix 5) form and these will be dealt with appropriately in line with this policy • Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy • Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs) • Liaising with other agencies and/or external services if necessary • Providing regular reports on online safety in school to the headteacher and/or governing board • Undertaking annual risk assessments that consider and reflect the risks pupils face • Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
All staff	• 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) and Online Safety Lead (OSL) are; 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 • Identify opportunities to thread online safety through all school activities as part of a • 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 (find out what appropriate filtering and monitoring systems are in place and how they keep children safe). • 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 – refer to the remotesafe.lgfl.net 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 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/OSL know • Receive regular updates from the DSL/OSL 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. • Understand your responsibility and those of others when it comes to filtering and monitoring and feedback to the Headteacher on any potential issues that arise
PSHE lead	• 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/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE. • Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach
Computing lead	• 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/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leads	• 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
Data Protection Officer (DPO) John Pearson Hicks	• Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
Data Manager Michaela McCadden	• To ensure that the data they manage is accurate and up-to-date • To ensure that all pupil data held on pupils on the school office machines have appropriate access controls in place (SIMs) • To keep the Head teacher up to date with additions or changes with use of the new subscribed system for DBS checks
The ICT manager: Andrew Canter	The ICT manager is responsible for: • Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material • Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly • A daily data backup is performed every evening to the LGFL-provided cloud storage service, 'Gridstore'. Additionally, a full physical backup is conducted weekly to a hard drive securely located at the school • Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files • Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy • Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
Pupils	• 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
All staff and volunteers	• All staff, including contractors and agency staff, and volunteers are responsible for: • Maintaining an understanding of this policy • Implementing this policy consistently • Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 4), and making sure that pupils follow the school's terms on acceptable use (appendices 2) • Knowing that the Designated Safeguarding Lead is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents or concerns regarding the failure of those systems or processes by promptly reporting to the DSL/ the Data Protection Officer/Chair Of Governors. This ensures that issues are addressed swiftly and effectively to maintain a safe online environment for all members of the school community. • Following the correct procedures by obtaining prior approval from the Designated Safeguarding Lead and then the ICT Manager if they need to bypass the filtering and monitoring systems for

	legitimate educational purposes, ensures that any temporary access is carefully managed and recorded to maintain the safety and integrity of the school's online environment. • Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy • Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy • Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
Parents/carers	Parents/carers are expected to: • Notify a member of staff or the headteacher of any concerns or queries regarding this policy • Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 2) Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites: What are the issues? – UK Safer Internet Centre Help and advice for parents/carers – Childnet Parents and carers resource sheet – Childnet
Visitors and members of the community	Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 4).

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 1**, pupils will be taught 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

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers via the school website.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

5. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6. Examining electronic devices

The headteacher, or member of SLT authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL or Deputy DLS’s.

- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation
- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

St Gabriel's recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St Gabriel's will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policy. Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

8. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 2). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 - 3.

6. Devise Usage

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

- **Pupils** in Year 6 are allowed to bring mobile phones in if they come to/from school by themselves. These must be handed in to the School Office during the day and must not be used/accessed during the school day under any circumstances. Any attempt to use a phone in school time without permission or to take illicit photographs or videos will lead to appropriate sanctions and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. No mobile phones are allowed in the EYFS at all. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Visitors to the EYFS must leave their phones at the office. 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 of staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. No phones are allowed in the EYFS at all.

Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office

7 Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software

Keeping operating systems up to date by promptly installing the latest update
Work devices must be used solely for work activities.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 4.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

8. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and/or staff code of conduct.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training

Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation

10. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. A Safeguarding Protection Concern form can be found in appendix 5.

This policy will be reviewed every year by the Computing lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

11. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

11. Contacts and references

CEOP (Child Exploitation and Online Protection Centre)**: www.ceop.police.uk**
Childline: www.childline.org.uk
Childnet**: www.childnet.com**
Kidsmart**: www.kidsmart.org.uk**
Think U Know website**: www.thinkuknow.co.uk**

12. Appendices

Appendix 1:' KS1 and KS2 Responsible use of the internet rules for children (AUP)

Appendix 2: 'Rules for the Responsible Use of the Internet' Poster.

Appendix 3: Request letter to parents asking for permission to use a photograph of their child on the school web site/class blog/

Appendix 4: Acceptable Use Policy for Staff, volunteers are outside agencies

Appendix 5: Acceptable Use Policy for parents/carers

Appendix 6: St Gabriel's School Safeguarding/Child Protection Recording Concerns

Appendix *1*

St Gabriel's C.E Primary School

Reception Rules for Keeping safe online and being a responsible internet user

- *I will always ask a trusted adult if I want to use the computers, tablets or cameras.*
- *I will only do the things that an adult has asked me to do on the computer.*
- *I will tell an adult if I see something on a screen that upsets me.*
- *I know personal things like my address and birthday should never be shared on the internet.*
- *I know I must never talk to strangers online.*
- *I know I should never meet someone in person that I have talked to on the internet without talking to a trusted adult about it first.*

Class signatures:

St Gabriel's C.E Primary School

KS1 Rules for Keeping safe online and being a responsible internet user

- *Always ask permission from a teacher to use the Internet.*
- *I always ask a teacher or trusted adult if I want to use the computers, tablets or cameras.*
- *I only open the activities that an adult has instructed or allowed me to use.*
- *I know that I must tell an adult if I see something on a screen that upsets me, or that I am unsure of.*
- *I keep my passwords safe and I will never use someone else's.*
- *I know personal information such as my address and birthday should never be shared online.*
- *I know I must never communicate with strangers online.*
- *I am always polite when I post to class blogs, use our email or other communication tools.*
- *Never arrange to meet someone in person that you have communicated with on the Internet without talking to your teacher or trusted adult about it first.*

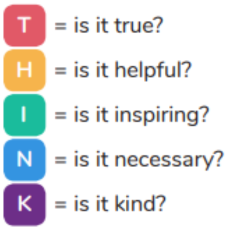
Class signatures:

St Gabriel's C.E Primary School

KS2 Rules for Keeping safe online and being a responsible internet user

- *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.*
- *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.*

Class signatures:



T = is it true?

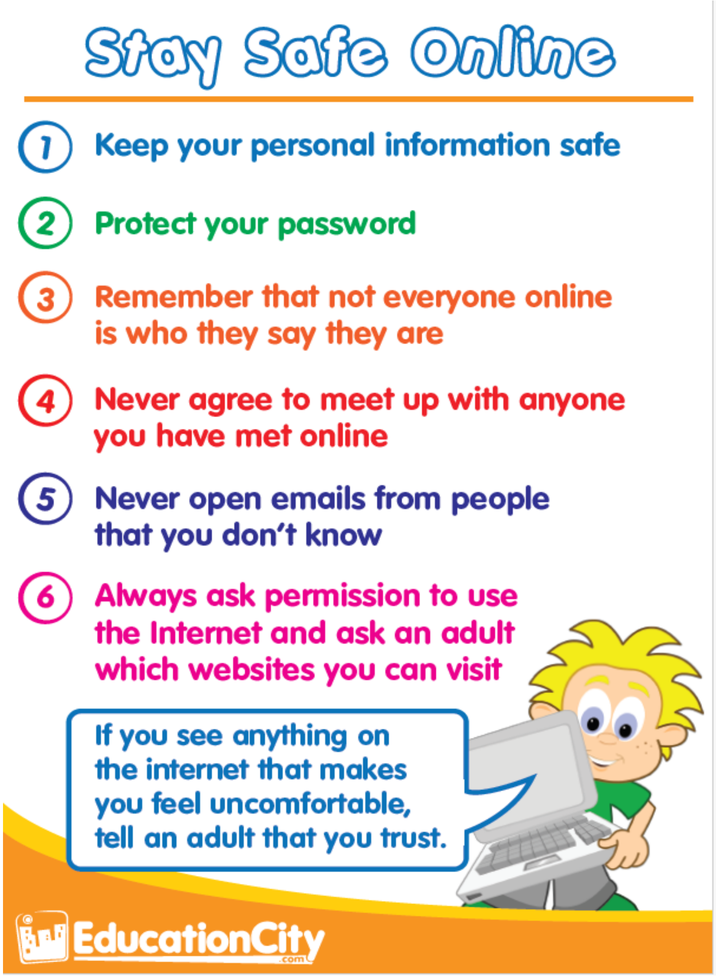
H = is it helpful?

I = is it inspiring?

N = is it necessary?

K = is it kind?

Appendix *2*

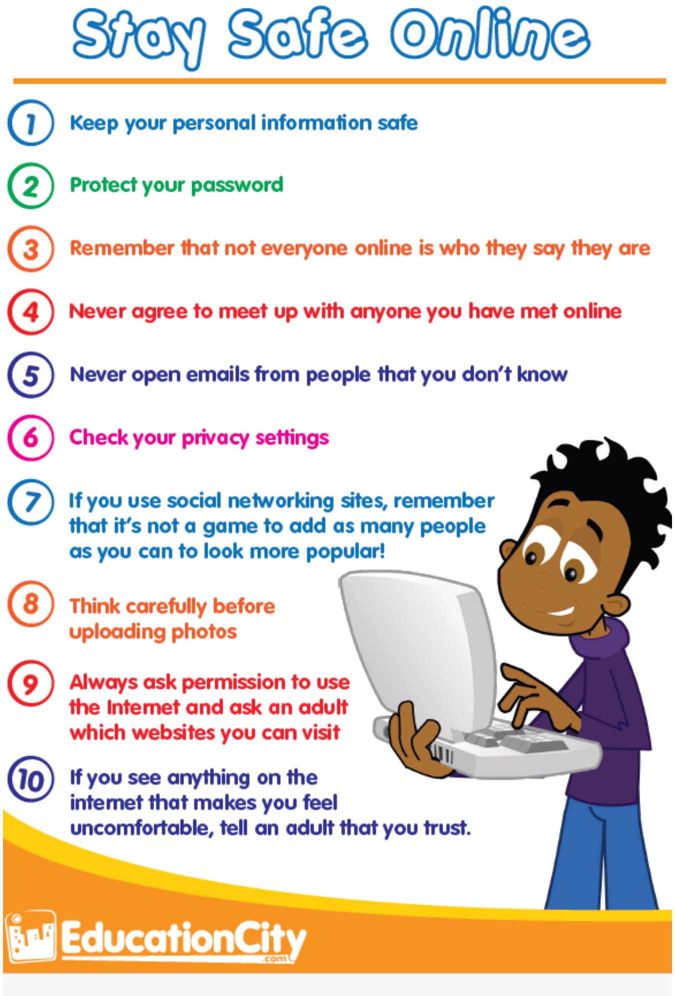


Stay Safe Online

1. Keep your personal information safe
2. Protect your password
3. Remember that not everyone online is who they say they are
4. Never agree to meet up with anyone you have met online
5. Never open emails from people that you don't know
6. Always ask permission to use the Internet and ask an adult which websites you can visit

If you see anything on the internet that makes you feel uncomfortable, tell an adult that you trust.

EducationCity.com



Stay Safe Online

1. Keep your personal information safe
2. Protect your password
3. Remember that not everyone online is who they say they are
4. Never agree to meet up with anyone you have met online
5. Never open emails from people that you don't know
6. Check your privacy settings
7. If you use social networking sites, remember that it's not a game to add as many people as you can to look more popular!
8. Think carefully before uploading photos
9. Always ask permission to use the Internet and ask an adult which websites you can visit
10. If you see anything on the internet that makes you feel uncomfortable, tell an adult that you trust.

EducationCity.com

Appendix 3:

St Gabriel's C.E. Primary School

Churchill Gardens Road
Pimlico, London
SW1V 3AG
Phone: 020 7186 0080

City of Westminster LA
Diocese of London
Headteacher: Rebecca Anson

Website: www.stgabrielsprimary.co.uk
Email: office@stgabrielsprimary.co.uk

September 2025

Dear Parent/Carer,

At St. Gabriel's primary school, we sometimes take photographs or films of pupils. We use these photos in the school's information booklet, on the school's website, in Newsletters, advertising, on social media and on display boards around school.

We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

If you change your mind at any time, you can let us know by emailing office@stqabrielsprimary.co.uk or, calling the school on 0207 186 0080.

If you have any other questions, please get in touch.

✂. . . . .

Please circle YES or NO beside each sentence below and return this form to school.

I give permission for the school to film or take photographs of my child. YES/NO

I give permission for photos or films of my child to be used on the school website. YES/NO

I give permission for photos of my child to be used in the school information booklet. YES/NO

I give permission for photos or films of my child to be used in internal displays and assemblies. YES/NO

I give permission for photos of my child to be used in school Newsletters. YES/NO

I give permission for photos of my child to be used in school advertising. YES/NO

I give permission for photos or films of my child to be used on the school social media accounts. YES/NO

If you do not consent to the school taking or using photos or films of your child please tick the box below.

I do **NOT** give permission for the school to take or use photos of my child. □

Child's name: ______________________________________ Class: ___________

Parent or carer's signature: ______________________________ Date: ____________

Appendix 4:

St Gabriel's CofE Primary School ICT User Agreement Policy: Staff, Volunteers, Governors & Contractors

1. Aims & Background

This ICT user agreement covers the use of all digital technologies while in school: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or Local Authority, or other information or systems processors. This ICT user agreement also covers school issued equipment (as logged on the asset register) when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school. This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute. The school regularly reviews and updates with the assistance of the DPO, all user agreement documents to ensure that they are consistent with current school policies as listed at the end of the agreement.

2. User Requirements

School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures being started. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

A) I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body in the line of my employment.
B) I will set strong passwords, following advice provided by the school or its ICT Manager. I will change it frequently.
C) I will not reveal my password(s) to anyone.
D) I will not use anyone else's password if they reveal it to me and will advise them to change it.
E) I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.
F) I will ensure all documents; data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols, and retention policy.
G) I will not engage in any online or other media activity that may compromise my professional responsibilities.
H) I will only use the schools approved email system(s) for any school business.
I) I will only use the approved method/s of communicating with pupils or parents/carers and will only communicate with them in a professional manner and on appropriate school business.
J) I will not support or promote extremist organisations, messages or individuals.
K) I will not give a voice or opportunity to extremist visitors with extremist views.
L) I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
M) I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the headteacher.
N) I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the School Office and/or ICT Manager.
O) I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
P) I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other malware systems.
Q) 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 or on any personal devices.
R) I will follow the school's policy on use of mobile phones / devices at school
S) 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.

T) I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. I will not identify students by name, or other personal information.
U) I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
V) I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two.
W) I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
X) I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
Y) I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.
Z) I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
AA) I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
BB) I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
CC) I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.
DD) I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
EE) I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
FF) I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
GG) Staff that have a teaching role only: I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

3. Links with Other Policies

I understand that this user agreement is linked to the schools:

- Freedom of information publication scheme
- Online and E-Safety Policy
- Email Security and Etiquette Guidance
- GDPR/Data Protection Policy
- Document Retention Policy
- Breach Management Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Safeguarding and Child Protection Policy

4. Agreement Form User Signature

I agree to abide by all the points above. I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ....
Date ....
Full Name .... (printed)
Job title / Role ....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role
Signature ....
Date...
Full Name .... (printed

Appendix 5

Acceptable Use Policy (AUP) for PARENTS AND CARERS What is an AUP?
We ask all children, young people and adults involved in the life of St Gabriel's C of E Primary School to sign an Acceptable Use* Policy (AUP), which is a document that 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). Your child has been taught the rules for being a responsible internet user and has signed these rules (an age appropriate AUP). You can view these rules on our website within the Online Safety Policy.

Why do we need an AUP?
These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe. We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community: "Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?
You can read St Gabriel's C of E Primary School full Online Safety Policy on our website. If you have any questions about this AUP or our approach to online safety, please speak to your child's teacher, a member of the SLT or our online safety lead, Sonia Bell.

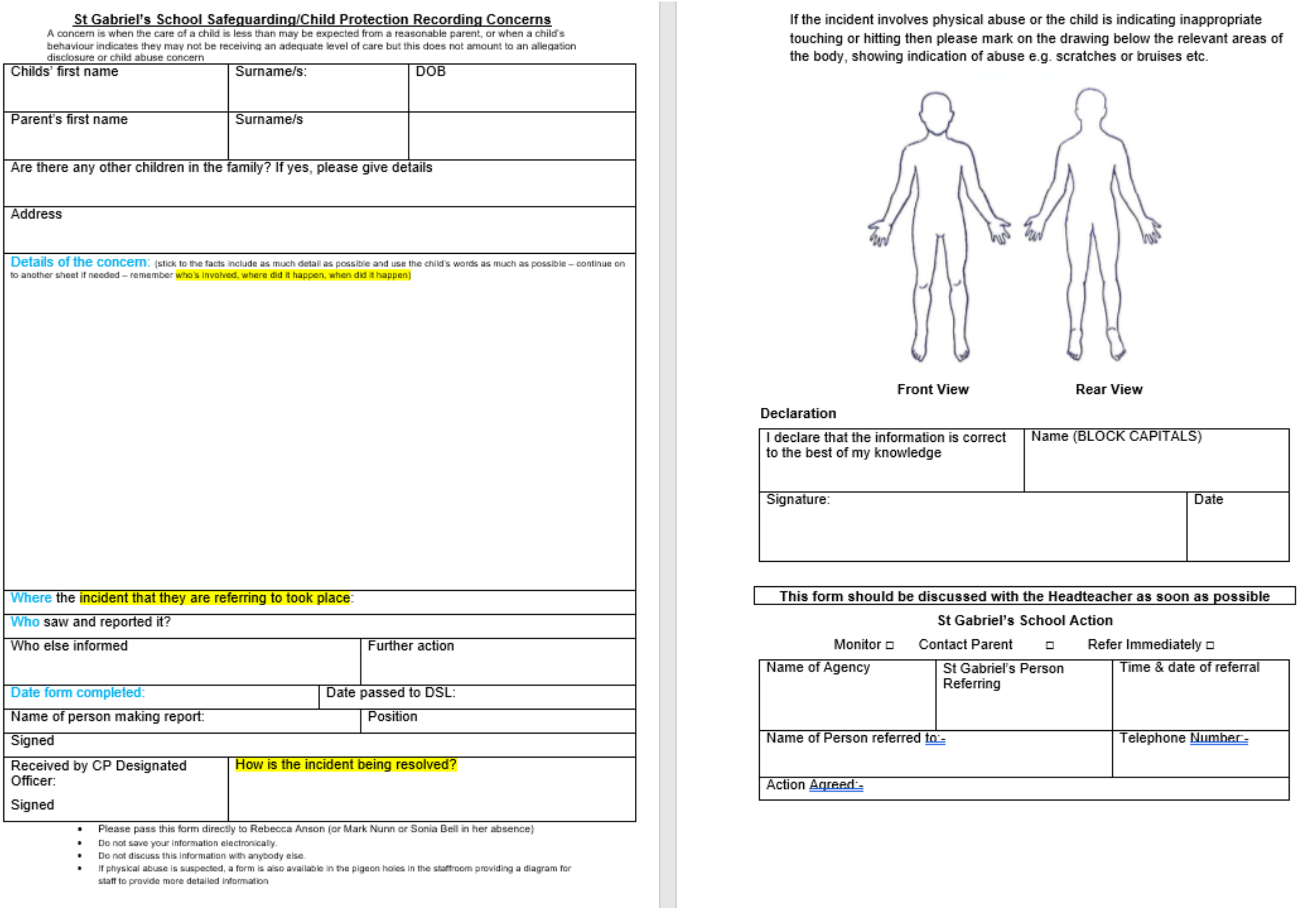
What am I agreeing to?

1. I understand that St Gabriel's C of E Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including 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 device use 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.
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 social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
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 (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. https://www.internetmatters.org/
9. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen on the school website and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
10.I can find out more about online safety at St Gabriel's C of E Primary School by reading the full Online Safety Policy found on the school website and can talk to my child's teacher, a member of the SLT or the e-safety lead

if I have any concerns about my child/ren’s use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood and agreed to this policy.
Signature/s: ____
Name/s of parent / guardian: ____
Parent / guardian of: ____
Date: ____

Appendix 6



St Gabriel’s School Safeguarding/Child Protection Recording Concerns

A concern is when the care of a child is less than may be expected from a reasonable parent, or when a child’s behaviour indicates they may not be receiving an adequate level of care but this does not amount to an allegation disclosure or child abuse concern

Childs’ first name	Surname/s:	DOB
Parent’s first name	Surname/s	
Are there any other children in the family? If yes, please give details		
Address		
Details of the concern: (stick to the facts include as much detail as possible and use the child’s words as much as possible – continue on to another sheet if needed – remember who’s involved, where did it happen, when did it happen)		
Where the incident that they are referring to took place:		
Who saw and reported it?		
Who else informed	Further action	
Date form completed:	Date passed to DSL:	
Name of person making report:	Position	
Signed		
Received by CP Designated Officer: Signed	How is the incident being resolved?	

- Please pass this form directly to Rebecca Anson (or Mark Nunn or Sonia Bell in her absence)
- Do not save your information electronically.
- Do not discuss this information with anybody else.
- If physical abuse is suspected, a form is also available in the pigeon holes in the staffroom providing a diagram for staff to provide more detailed information

If the incident involves physical abuse or the child is indicating inappropriate touching or hitting then please mark on the drawing below the relevant areas of the body, showing indication of abuse e.g. scratches or bruises etc.

Front View

Rear View

Declaration

I declare that the information is correct to the best of my knowledge	Name (BLOCK CAPITALS)	
Signature:		Date

This form should be discussed with the Headteacher as soon as possible

St Gabriel’s School Action

Monitor □ Contact Parent □ Refer Immediately □

Name of Agency	St Gabriel’s Person Referring	Time & date of referral
Name of Person referred to:-		Telephone Number:-
Action Agreed:-		