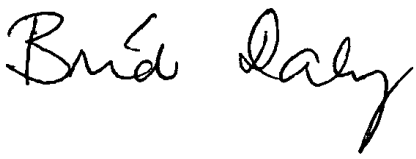
FEDERATION OF

St Peter's and St Gildas'

INFANT AND JUNIOR SCHOOLS

Online Safety & AUP's Policy

Updated by	Sinead O'Brien
Governor Responsible	Brid Daly
Last Reviewed	September 2020
Policy Date	September 2021
Review period	Annual
Signed	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 them 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 scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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
- 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 takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 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 co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Brid Daly**

All governors will:

- Ensure that 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 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and DDSL 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 ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- 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 child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring 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

This list is not intended to be exhaustive.

3.4 The ICT manager/School Business Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Regular monitoring of school IT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring 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'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 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 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

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

- 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 online 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 is shared and used online
- 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 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.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

If parents 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.

6. Cyber-bullying

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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 are encouraged 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 classes.

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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Independent travellers and pupils in year 6 may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Playtimes
- Clubs before or after school, or any other activities organised by the school

All devices should be handed to the **classteacher** at the start of the day

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device or being barred from bringing it into school

9. 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from DSL/SBM

10. 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 policy on behaviour. 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/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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

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, 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 the risks up
- 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 & DDSL 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on MyConcern.

This policy will be reviewed every year by the Designated Safeguarding 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.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Complaints procedure
- Staff Code of Conduct

Appendix 1- Acceptable Use Agreement EYFS & KS1

To stay **SAFE online and on my devices**:

1. I only **USE** devices or apps, sites or games if a trusted adult says so.
2. I **ASK** for help if I'm stuck or not sure.
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused.
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.
5. I look out for my **FRIENDS** and tell someone if they need help.
6. I **KNOW** people online aren't always who they say they are.
7. Anything I do online can be shared and might stay online **FOREVER.**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to.
9. I don't change **CLOTHES** in front of a camera.
10. I always check before **SHARING** personal information.
11. I am **KIND** and polite to everyone.

My trusted adults are:

_____ **at school** _____ **at home**

I also trust _____

Appendix 1- Acceptable Use Agreement KS2

1. ***I learn online*** – I use the school's internet, cloud platforms and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or pop-ups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it with others. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult: at school that includes: _____ Outside school, my trusted adults are: _____

Signed: _____ **Date: _____**

Appendix 1- Acceptable Use Agreement Parents/Carers

What is an Acceptable Use Agreement?

We ask all children, young people and adults involved in the life of St Peter's and St Gildas' to sign an Acceptable Use Agreement, 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 the school site and outside of school).

Your child also signs an agreement which you need to discuss with them before they sign.

Why do we need an Acceptable Use Agreement?

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."

What am I agreeing to?

1. I understand that the Federation of St. Peter's and St. Gildas' 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. Student should use devices at home 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 guidance and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's Digital Images Consent Policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media without permission 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, but it will only do so publicly if I have given my consent.

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.
9. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
10. I understand and support the commitments made by my child in their Acceptable Use Agreement which s/he has signed. I understand that s/he will be subject to sanctions if s/he does not follow these rules.
11. 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 will contact my child's class teacher or the school offices admin@st-peter-in-chainsrc.haringey.sch.uk or admin@st-gildas.haringey.sch.uk

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

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

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____
~~~~~~~~~~~~~~~~

Appendix 2

Use of Images statement

Aims of this statement

The Federation of St Peter's and St Gildas' believes that strong safeguarding principles are essential to ensuring our pupils are able to learn in a safe, secure and welcoming environment that enables them to reach their full potential.

The purpose of this policy is to:

- protect children and young people who take part in lessons, services, events and activities, specifically those where photographs and videos may be taken
- set out the overarching principles that guide our approach to photographs/videos being taken of children and young people during our events and activities
- to ensure that we operate in line with our values and within the law when creating, using and sharing images of children and young people.

This policy statement applies to all staff, volunteers and other adults associated with The Federation of St Peter's and St Gildas' schools.

Legal framework

This statement has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of key legislation and guidance is available on NSPCC Learning:

online abuse legislation and guidance

Child protection legislation and guidance

We believe that:

- children and young people should never experience abuse of any kind
- we have a responsibility to promote the welfare of all children and young people and to take, share and use images of children safely.

We recognise that:

- sharing photographs and films of our activities can help us celebrate the successes and achievements of our children and young people, provide a record of our activities and raise awareness of our organisation
- the welfare of the children and young people taking part in our activities is paramount
- children, their parents and carers have a right to decide whether their images are taken and how these may be used, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation
- consent to take images of children is only meaningful when children, their parents and carers understand how the images will be used and stored, and are fully aware of the potential risks associated with the use and distribution of these images
- there are potential risks associated with sharing images of children online.

We will seek to keep children and young people safe by:

- always asking for written consent from a child and their parents or carers before taking and using a child's image
- always explaining what images will be used for, how they will be stored and what potential risks are associated with sharing images of children
- making it clear that if a child or their family withdraw consent for an image to be shared, it may not be possible to delete images that have already been shared or published
- never publishing personal information about individual children.
- making sure children, their parents and carers understand how images of children will be securely stored and for how long (including how we will control access to the images and their associated information)
- reducing the risk of images being copied and used inappropriately by:
- only using images of children in appropriate clothing (including safety wear if necessary)
- avoiding full face and body shots of children taking part in activities such as swimming where there may be a heightened risk of images being misused
- using images that positively reflect young people's involvement in the activity.

We will also develop a procedure for reporting the abuse or misuse of images of children as part of our child protection procedures. We will ensure everyone involved in our organisation knows the procedures to follow to keep children safe.

Photography and/or filming for personal use

When children themselves, parents, carers or spectators are taking photographs or filming at our school events and the images are for personal use, we will publish guidance about image sharing in the event programmes and/or announce details of our photography policy before the start of the event. This includes:

- reminding parents, carers and children that they need to give consent for St Peter's and St Gildas' to take and use their images

- asking for photos taken during the event not to be shared on social media or asking people to gain permission from children, their parents and carers before sharing photographs and videos that include them
- recommending that people check the privacy settings of their social media account to understand who else will be able to view any images they share
- reminding children, parents and carers who they can talk to if they have any concerns about images being shared.

Photography and/or filming for St Peter's and St Gildas' use

We recognise that teaching staff may use photography and filming as an aid all lessons. However, this should only be done with St Peter's and St Gildas' SLT permission and using our school equipment where possible. Where this is not possible images must never be stored on personal devices.

Children, young people, parents and carers must also be made aware that photography and filming is part of the programme and give written consent.

If we hire a photographer for one of our events, we will seek to keep children and young people safe by:

- providing the photographer with a clear brief about appropriate content and behaviour
- ensuring the photographer wears identification at all times
- informing children, their parents and carers that a photographer will be at the event and ensuring they give written consent to images which feature their child being taken and shared
- not allowing the photographer to have unsupervised access to children
- not allowing the photographer to carry out sessions outside the event or at a child's home
- reporting concerns regarding inappropriate or intrusive photography following our child protection procedures.

Photography and/or filming for wider use

If people such as local journalists, professional photographers or students wish to record one of our events and share the images professionally or in the wider world, they should seek permission in advance.

They should provide:

- the name and address of the person using the camera
- the names of children they wish to take images of (if possible)
- the reason for taking the images and/or what the images will be used for
- a signed declaration that the information provided is valid and that the images will only be used for the reasons given.

St Peter's and St Gildas' will verify these details and decide whether to grant permission for photographs/films to be taken. We will seek consent from the children who are the intended subjects of the images and their parents and inform the photographer of anyone who does not give consent.

At the event we will inform children, parents and carers that an external photographer is present and ensure the photographer is easily identifiable, for example by issuing them with a coloured identification badge.

If St Peter's and St Gildas' staff are concerned that someone unknown to us is using their sessions for photography or filming purposes, we will ask them to leave and

(depending on the nature of the concerns) follow our child protection procedures.

If consent to take photographs is not given

If children, parents and/or carers do not consent to photographs being taken, we will respect their wishes. We will agree in advance how they would like to be identified so the photographer knows not to take pictures of them, and ensure this is done in a way that does not single out the child or make them feel isolated.

We will never exclude a child from an activity because we do not have consent to take their photograph.

Storing images

We will store photographs and videos of children securely, in accordance with our safeguarding policy and data protection law.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and child protection policy and procedures.
- Code of conduct for staff and volunteers.
- Online safety policy and procedures for responding to concerns about online abuse.

This policy was implemented on: September 2021

This policy will be reviewed on: September 2022

Signed: ……

Chair of Governors The Federation of St Peter's and St Gildas' Schools

Date: ……