QEGSMAT

St. John's CE Primary School
Wetley Rocks

Online Safety Policy

"Shine like the star you are."

"You are the light of the world. A town built on a hill cannot be hidden.
15 Neither do people light a lamp and put it under a bowl, instead they put it on its stand, and it gives light to everyone in the house. In the same way, let your light shine before others, that they may see your good deeds and glorify your Father in heaven."
Matthew 5:14-16

Our Values

***S*trength:** *have the strength to stand up for what is right. Be a courageous advocate.*
***H*ope:** *to be people of hope. Have hope when times are dark and difficult. Keep positive and be resilient – there is light at the end of the tunnel.*
***I*ndividuality:** *embrace and celebrate our differences. God made us all unique and this is a very special thing.*
***N*uture:** *cherish, care for, encourage and protect everything in God's world - including yourself.*
***E*xcel:** *fulfil your God given potential; be the best you can be. Shine like the star you are.*

Introduction/Key people and dates:

Head Teacher	Sarah Stone
Designated Safeguarding Lead	Sarah Stone
Online Safety Lead	Rebecca Poynton
Safeguarding Link Governor	Cheryl Tunstall
IT support Provider	LINK ICT
Data Protection Lead	Sarah Stone
Computing Lead	Rebecca Poynton
PHSE Lead	Jo Graham

What is this policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE) and other statutory documents; it sits alongside the school's statutory Safeguarding and Child Protection Policy. Any issues and concerns with online safety must follow the school's safeguarding procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, staff, Governors, pupils and parents are involved in writing and reviewing the policy. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-today practice. Acceptable Use Agreements (see appendices) for different stakeholders help with this. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

We have a named online safety leader at St John's Primary School (see above); this person is not the designated safeguarding lead (DSL), but KCSIE makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." The DSL and Online Safety Lead work together to ensure online safety is adhered to. When unsafe online safety are brought to the school's notice, both the DSL and Online Safety Lead agree an appropriate way forward in-line with procedures outlined in both the Trust Child Protection Policy and Online Safety Policy.

What are the main online safety risks today?

Online safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commercialism These areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three. For many years, online safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, harmful sexual behaviours and coerced nudity via live streaming. Commercialism is now becoming a bigger problem as children have access to sites with hidden costs. Contact and conduct of course also remain important challenges to address.

CORE	**Content** Child as recipient	**Contact** Child as participant	**Conduct** Child as actor	**Contract** Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Children Online: Research and Evidence 2023

How will this policy be communicated?

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

- Posted on the school website.
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff).
- For temporary and supply staff, school will provide a key points leaflet to enable them to carry out their online safeguarding duties.
- Integral to safeguarding updates and training for all staff (especially in September refreshers).
- Clearly reflected in the Acceptable Use Agreement (AUA) for staff, volunteers, contractors, Governors and pupils who have access to our digital technology, networks and systems whether on site or remotely.
- AUA issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review.
- Teachers inform pupils via the curriculum.

Overview

Aims

This policy aims to:

- Set out expectations for all St John's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    1. For the protection and benefit of the children and young people in their care.
    2. For their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    3. For the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which, in school, online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Positive Behaviour Policy).

Further help and support

Internal school channels should always be followed first for reporting and support, as documented in in line with the Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the Headteacher will handle referrals to the LA designated officer (LADO). The local authority or third-party support organisations we work with may also have advisors to offer general support. This policy applies to all members of the St John's community (including staff, Governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely.

Roles and responsibilities

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

Head teacher Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance.
- Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Governors to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including mitigating the risk of children being radicalised.
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory DfE requirements.

Designated Safeguarding Lead/Online Safety Lead Key responsibilities:

The DSL can delegate certain online safety duties, e.g. to the online safety leader, but not the overall responsibility;

- The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).
- As the online safety leader is not the named DSL, or deputy DSL, we will ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure an effective approach to online safety [that] empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
- Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children.
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the Head teacher, DPO and Governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.

- Stay up to date with the latest trends in online safety. The website has a link to Wake Up Wednesday from the National Online Safety Website. This allows parents to access help and support for the most common and well used apps and websites.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Agreements) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum and beyond.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with SLT and the designated safeguarding governor and deputy to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss appropriate physical and technical filtering and monitoring with Governors, and ensure staff are aware.
- Ensure the Department for Education guidance on harmful sexual behaviours, sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff:

1) All staff must read KCSIE Part 1 and all those working with children Annex A and B.
2) We also advise all staff to be aware of Annex C (online safety)
3) Cascade knowledge of risks and opportunities throughout the organisation.

<u>Governing Body, led by Safeguarding Link Governor Key responsibilities</u>

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCCIS) Online safety in schools and colleges:
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety leader / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.

- As the online safety leader is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Work with the DPO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE at the start of each new academic year; SLT and all working directly with children have read Annex A and B; check that Annex C on Online Safety reflects practice in the school.
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated in line with advice from the QEGSMAT
- Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

All staff Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are in school.
- Read Part 1, Annex A, B and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A and B for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff acceptable use agreement.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

- Encourage pupils/students to follow their acceptable use agreement, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying, harmful sexual behaviours and sexual harassment even if appears to be low-level (the DSL will update staff of the latest guidance from the DfE)
- Be aware that you may 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 safety issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE Leader Key responsibilities from September 2020

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.

Computing Curriculum Leader Key responsibilities:

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

Subject/Aspect Leaders Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCCIS framework Education for a Connected World 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.

IT Support Providers Key responsibilities LINK ICT:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role. Staff will be informed during relevant training days.
- Work closely with the designated safeguarding lead / online safety lead / data protection lead to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc .
- Support and advice on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school's online security and technical procedures on a yearly basis.
- Report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Head teacher to ensure the school website meets statutory DfE requirements (see appendices for website audit document)

Data Protection Lead Key responsibilities:

Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools', especially this quote from the latter document:

- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing,

appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding."

- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'
- Work with the DSL, Headteacher and Governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.
- Liaise with the DPO (outside agency) for advice and guidance about the above.

Pupils Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use agreement and review this at the beginning of each key stage.
- Read the appropriate AUA annually.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- 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 agreements provide guidelines as to how to behave out of school when using online devices.
- Be aware of the benefits/opportunities and risks/dangers of the online world (at an age appropriate level) and know who to talk to at school or outside school if there are problems

Volunteers and contractors Key responsibilities:

- Read and understand safeguarding polices.
- Report any concerns, no matter how small, to the designated safety lead / online safety leader.
- Model safe, responsible and professional behaviours in their own use of technology.

Parents/carers Key responsibilities:

- Read, sign and promote the school's parental acceptable use agreement (AUA) and read the pupil AUA and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Governors, contractors, pupils or other parents/carers.

Education and curriculum

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

- PSHE
- Relationships and Health Education
- Computing

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

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

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

At St John's Primary School & Nursery, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCCIS (the UK Council for Child Internet Safety - soon to become UKCIS as no longer solely for children). Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of self-image and identity, online relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership.

Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding as well as being a curriculum strand of Computing, PSHE and statutory Health and Relationships Education.

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

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

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

Safeguarding and Child Protection Policy.

- Positive Behaviour Policy.
- Acceptable Use Agreements.
- Prevent Policy within the overall safeguarding policy.
- Data Protection Policy.

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's policies. Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the Whistleblowing Policy. The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, National Crime Agency - Child Exploitation and Online Protection (NCA CEOP), Prevent Officer, Police, Internet Watch Foundation (IWF).

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

Actions where there are concerns about a child

As outlined previously, online safety concerns are no different to any other safeguarding concern. If you are concerned, use the following guidance:

If you're concerned about a child:

Report your concern immediately to a safeguarding member of staff in person.

If you believe the child to be at risk of immediate harm, this must be **reported to the police on 999 or 101**.

Once you have reported to the police, please contact Staffordshire Children's Advice and Support Service (SCAS / First Response / 'Front Door'): **0300 1118007 Option 1**

Out of hours

Outside of the hours above, or on weekends and bank holidays, please contact the **Emergency Duty Team: 0345 604 2886**.

If you're concerned about a professional working with a child:

Any allegation / low level concern regarding a member of staff, a child's foster carer or a volunteer should **be reported immediately to the Head teacher** (please see St. John's Safeguarding Policy Appendix 3 / KCSIE guidance for further information). If an allegation is made about the Head teacher, you should pass this information to the Chair of the Governing Body.

School Contacts:

Designated Safeguarding Lead (DSL): Sarah Stone / Head teacher's office / sstone@st-johns-wetleyrocks.staffs.sch.uk

Deputy Designated Safeguarding Leads (DDSL):

Steph Loton (Yr 2) / sloton@st-johns-wetleyrocks.staffs.sch.uk

Emily Rushton (Yr 3) / erushton@st-johns-wetleyrocks.staffs.sch.uk

Safeguarding Governor: Mrs Cheryl Tunstall / cheryl.tunstall@st-johns-wetleyrocks.staffs.sch.uk

Mental Health Lead: Mrs Jo Graham / jgraham@st-johns-wetleyrocks.staffs.sch.uk

Pastoral Support Lead: Mrs Julie Simcock / jsimcock@st-johns-wetleyrocks.staffs.sch.uk

Alternatively, you can contact the LADO (Local Authority Designated Officer): **0300 111 8007.**

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

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media. These are defined in the relevant Acceptable Use Agreement. Where pupils contravene these rules, the school positive behaviour policy will be applied. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology.

The Acceptable Use Agreement also provides guidance for how to behave when using online devices out of school.

Social media incidents

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, St John's Primary School will request that the post be deleted and will expect this to be actioned promptly. We would advise staff, parents and pupils of follow up actions if necessary. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The school has a Parent Code of Conduct policy which also runs alongside this section of the policy.

With regard to social media incidents, parents have access to Parent Code of Conduct policy and staff are governed by the Acceptable Use polices as outlined by QEGSMAT.

Data protection and data security

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.

Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding. All pupils, staff, Governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements

Appropriate filtering and monitoring

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

At St John's Primary School, Link ICT maintain and update all our ICT systems. We currently have RM and Smoothwall which filters and blocks inappropriate content. We also have Securus monitoring

systems supplied by ENTRUST Education Services. Securus is monitored on a weekly basis by the ICT lead.

Within KS1 we use the Swiggle Search engine so that the younger children can block inappropriate content immediately. It give them the option to put a hand over the screen and tell a teacher.

Email

Both pupils and staff have access to their own personal one drive account and email.

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

• Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

School website

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

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with the staff in charge of updating the website. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).
- Only photos and videos of pupils whose parents have given permission should be used on the website. This list is in the class red folders.

Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning. This school adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service. We use the following cloud platforms: Microsoft's Office 365. For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training help to keep staff and pupils safe, and to avoid incidents. Staff are prompted regularly to change their passwords. Link ICT manage our systems and advise us on current policy and procedure.

The data protection officer and online safety leader analyse and document systems and procedures before they are implemented, and regularly review them. The following principles apply:

- Privacy statements inform parents when and what sort of data is stored in the cloud
- Regular training ensures all staff understand sharing functionality
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them). All staff are governed by their contract of employment and the school's Acceptable Use Agreement, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At St John's Primary, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices and/or cloud services.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy. Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. We encourage young people to think about their online reputation and digital footprint and also advise parents and carers to be good adult role models by not oversharing. Pupils are taught about how images can be manipulated and also taught to consider how to publish for a wide range of audiences which might include Governors, parents or younger children. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make personal information public. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse

Social media

St John's Primary School's Social Media presence works on the principle that if we don't manage our social media reputation, someone else will. Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online

Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism .

Staff, pupils' and parents' Social Media presence

Social media (including here; all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. We expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. Please see our Parent Code of Conduct Policy on the website. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups. If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve). Many social media platforms have a minimum age of 13 years, but the school frequently deals with issues arising on social media with pupils/students under the age of 13 years. We ask parents to respect age ratings on social 21 media platforms wherever possible and not encourage or condone underage use.

It is worth noting that, following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise.

Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults. Parents can best support this by talking with their children about the apps, sites and games in use and setting limits on with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Guidance for parents who want to film, photograph or stream school events.

This guidance applies to all video or audio capture of staff and pupils, both in and out of school. It applies to sporting events, parents' evenings, plays, assemblies, school trips and any other school event or gathering, whether on school premises or beyond. We appreciate that families will treasure photographic/video memories, and the general rule is that parents and carers may take photos and videos of the children in their care, for personal use only. **There may be rare exceptions to this, and we will let you know in advance of particular events where no filming etc is possible. Thank you for your understanding.**

Live streaming, whether public or private, cannot be permitted and we request that you do not use any streaming platforms or 'live' features (e.g. Facebook Live) to stream events/circumstances as they occur. You may be asked to leave the premises or event if this takes place. When you capture

footage or still images of your children, there is a strong possibility that other children will also be visible or audible. For this reason, no such content should be shared publicly. You will have seen other parents share videos of school plays on social media, but this does not make it advisable or acceptable. There are several important reasons for this:

- Some children are deemed at risk by local authority safeguarding and child protection authorities; their image must never be put online for their own protection. You are very unlikely to know who these children are. Others may have complex family backgrounds which mean that sharing their image could have unforeseen consequence. There is the real possibility you could endanger a child by sharing their image in an identifiable context (e.g. where the school is easy to identify and locate).

- Express consent is needed from parents to comply with data protection legislation, which is being enhanced under GDPR and the new Data Protection Bill. Sharing could otherwise potentially incur fines for contravention of data protection rules.

- Some families may object for religious or cultural reasons, or simply for reasons of personal privacy.

- Sharing images of children in school uniform helps identify them so should not be done unless avoidable.

- We encourage young people at our school to think about their online reputation and digital footprint: online photos and videos do not simply disappear when we delete them from our accounts. Help us be good adult role models by not oversharing (or providing embarrassment in later life).

Where possible, we will take appropriate staged group shots of pupils whose parents/carers have given appropriate photographic permissions and make these available to you. Equally, and again wherever possible, we will ensure there is time for parents to take photographs of their own children for example by approaching the stage after a performance. The same provisions apply here as stated above. We want you to enjoy school events and activities with your child, so why not just sit back, enjoy the memories and allow others to do so too? Remember, your child wants to see you looking at them, not at your phone.

Personal devices for staff, pupils and visitors.

Please see our Bring Your Own Device Policy.

Trips / events away from school

For school trips/events away from school, teachers may need to use their personal phone in an emergency and will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number. They will report any such communication to the Headteacher. On trips and residential it may be necessary for staff members to take photographs and/or videos of pupils on their own personal mobile phones, so that they can be more easily shared with parents; for example, via Facebook.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them, have a statutory power to search pupils and their property on school premises. This includes the content of mobile phones and other devices, for

example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.