All Saints CE Primary School & Nursery

Nurturing, Resilience & Achievement for all!

Online Safety Policy

Date written:	January 2025
Date adopted/reviewed:	May 2025
Review schedule:	Biennially
Policy Area:	Curriculum

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, 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 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 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
- 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 body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will ensure the safeguarding governor as part of safeguarding visits monitors online safety.

The governor responsible for safeguarding is Steve Hammond.

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 (Appendices 3 & 4)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure 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
- Do all that they reasonably can to limit children's exposure to the risks identified in the 4C's from the school's IT system. The governing body will ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- The governing body will consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

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 designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

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
- Working with the headteacher, ICT manager and other staff, as necessary, to ensure the appropriate filtering and monitoring systems are in place and reviewed regularly
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy
- Ensuring that any online safety incidents are logged in line with the child protection and safeguarding policy (cause for concern forms)
- 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
- 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

3.4 The ICT 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
- Conducting a full security check and monitoring the school's ICT systems
- Alongside the service provider blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 (Appendices 1, 3 & 4), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged in line with the child protection and safeguarding policy (cause for concern forms)
- 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 and carers

Parents and carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child understands 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

3.7 Pupils

Pupils are expected to:

- Adhere to the Acceptable use agreement
- Seek help from school staff if they have any concerns
- Report online safety incidents and concerns

3.8 Visitors, hirers and members of the community

Visitors, hirers 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 (Appendices 1 & 3).

4. Educating pupils about online safety

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

All schools must teach:

- Relationships education and health education in primary 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 information via our website This policy will also be shared with parents.

Online safety may also be covered during parents' evenings and parent workshops

The school will let parents 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 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 1 person or group by another person or group, where the relationship involves an imbalance of power.

Types of cyber bullying may include:

Child on child sexual abuse and harassment

Threatening, facilitating or encouraging sexual violence. Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks. Sexualised online bullying, e.g. sexual jokes or taunts. Unwanted and unsolicited sexual comments and messages. Consensual or non-consensual sharing of sexualised imagery. Abuse between young people in intimate relationships online).

Grooming and exploitation

Where an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing.

Child sexual exploitation (CSE) and child criminal exploitation (CCE). CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Radicalisation, the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Online hoaxes and harmful online challenges

An online hoax is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

'Harmful online challenges' refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. An online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly because of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

6.2 Preventing and addressing cyber-bullying

All Saints School has a zero-tolerance approach to any forms of 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. 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.

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.

6.3 Examining electronic devices

The headteacher, and any member of staff 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 headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil’s cooperation

Authorised staff members may examine 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 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 if 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 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 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

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 and IT systems in school

All users (pupils, staff, volunteers, parents and governors) are expected to read and understand the acceptable use conditions for using the school's IT systems and the internet (Appendices 1 to 3). Staff, governors and volunteers that will have access to IT systems in school are required to sign a specific Acceptable Use Agreement (Appendix 3) to ensure they are clear on their responsibilities, and should be aware of the guidance in Appendix 4. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant (Appendix 3).

Importantly, anyone using the school's IT systems, internet or online services will be deemed to have automatically agreed to the Acceptable Use Agreements in place at the time (Appendices 1 to 3 of this policy) regardless of if they have signed a physical copy of the conditions or not.

This includes parents of children attending All Saints CE Primary School, unless parents have made an appointment to discuss and opt their child out of the agreement. In the case a child has been opted out by their parents, the school may restrict their access to the school's IT systems.

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 to 3.

Appendix 4 contains specific guidance for staff which outlines the expected use of school IT systems:

- Use of email
- Visiting websites and downloading information
- Storage of images
- Use of personal mobile devices (including phones)
- New technologies and online services

8. Mobile devices

We believe mobile devices can form part of a broad and balanced curriculum and can support positive experiences for learning. However, pupils at primary school age need explicitly teaching about how to use mobile devices safely and healthily, and much of their learning can be completed successfully without need for mobile devices. Although they can be a positive opportunity for learning, without effective boundaries and safeguards, mobile devices can have a significant negative impact on the children's social interaction, development and learning. Therefore, we do not encourage pupils at primary age to have a personal mobile device (e.g. smart phone, smart watch etc.).

To this end, we encourage parents to be mindful of the impact a mobile device can have on their child and ensure if they choose to provide a device, they have put appropriate safeguards in place to protect their children. The school is required to follow Child Protection procedures where there are concerns about any child's access to inappropriate material, including under-age apps, videos and other online content. As a guiding principle, almost all popular social media apps have a minimum user age of 13. No child in our school is old enough to have their own accounts for these apps/online resources.

Where pupils do access learning online in school, we will provide devices and materials appropriate to the activity. This ensures pupils access devices and material which are appropriate to their age and the educational purpose intended. For the avoidance of doubt, we include smart watches with the facility to make/receive calls or take/record photos and audio recordings in the definition of mobile devices.

Personal mobile devices in school

Only those children in Year 5 and 6 walking to and from school by themselves are permitted to bring mobile devices to school, and only if it is deemed essential by their parents. Children in other year groups must not bring in their own devices for any reason and if they have them should leave them at home.

No pupils are permitted to use mobile devices whilst in school (or care of school) at any time. This includes during:

- Lessons
- Break times (including lunch time)
- Trips and other offsite activities during the school day
- Clubs before or after school, or any other activities organised by the school (on or off school premises)

All devices must be switched off while on the school grounds and handed in to the class teacher on entry to school. They can be retrieved at the end of the school day. School will accept no responsibility for loss or damage to any personal devices brought in by pupils, parents or staff.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's behaviour policy, which may result in the confiscation/banning of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their work-provided 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, hash-tag, 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 (all work provided devices have this as standard)
- Keeping operating systems up to date by always installing 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 Appendices 1, 3 & 4.

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 the ICT manager as soon as possible.

Using personal devices to access school systems

All staff are encouraged to use school provided devices as far as possible. However, we recognise that many staff may need or choose to use personal mobile devices or laptops to access school online systems. In these cases, they must ensure that the above steps are taken to ensure any access to online systems or work-related files are secure and protected from unauthorised access.

In addition, personal devices belonging to staff, including visitors, parents and agency staff, must only be used in designated areas and never in the presence of pupils without written permission from the Headteacher.

Music Teachers – we recognise that Herts Music Service (HMS) and other music teaching staff may be required to use personal devices as part of their teaching in school and as such, will be used in the presence of pupils. HMS provides assurance that all their staff will follow strict policies and only use their personal devices in schools for this purpose. In our school, this use will be permitted while staff follow HMS policies.

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 behaviour and child protection policies. 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.

Where a **visitor / contractor / parent** misuses a school ICT system, the internet or a personal device contrary to the acceptable use policy, they will be reminded of their responsibility to follow the acceptable use policy and asked to cease any misuse immediately. Depending on the individual circumstances, nature and seriousness of the specific incident, the school may need to follow procedures set out in child protection policies.

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 online safety and links to child protection and safeguarding.

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.

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 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** 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 about 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety as per the school's child protection and safeguarding policy.

This policy will be reviewed every two years by the head teacher or member of staff delegated this responsibility. The policy will be shared with the governing body.

13. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: Acceptable Use Table

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below. Additionally, all staff are required to sign a specific Acceptable User Agreement (Appendix 3) and should be aware of the guidance in Appendix 4. Please also see Section 7 of the Online Safety Policy.

The acceptable use as defined in our policy will be communicated/re-enforced through:

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- parental workshops and sessions
- computing and PSHE lessons
- Collective Worship and assemblies
- school website
- peer support

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990):	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	- Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information ***here***					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

The following activities outline acceptable use by user type:

User activities:	Staff and other adults:				Learners:			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff (due to their role)	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission / awareness
Online Gaming	X							
Online shopping				X				
File sharing (internal using school systems only e.g. Teams, Google Classroom)		X				X		
File sharing (external)		X			X			
Social media (school based)				X	X			
Social media (personal)			X (Staff Room)		X			
Messaging / chat			X		X			
Entertainment streaming (e.g. Netflix, Disney+ etc.)	X				X			
Use of video broadcasting (e.g. YouTube, Twitch, TikTok etc.)	X				X			
Use of personal mobile phones for learning at school				X	X			

User activities:	Staff and other adults:				Learners:			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff (due to their role)	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission / awareness
Personal mobile phones may be brought to school		X			X			X (Y5 & 6 only)
Use of personal mobile phones in social times at school			X (Staff room)		X			
Taking photos on personal mobile phones/cameras for learning activities	X				X			
Taking photos on personal mobile phones/cameras for other reasons.	X				X			
Uploading photos, videos, sounds or words that could upset another member of our school (now or in the future)	X				X			
Use of other personal devices in school (e.g. tablets, gaming devices etc.)	X				X			
Use of personal email on school network/WiFi (with awareness it may be monitored)			X		X			
Use of school email for personal emails	X				X			
Use of school WiFi (a monitored guest network is available for external devices)		X						X
Share confidential information about the school,			X		X			
Sharing personal information (e.g. home address, personal phone number etc.)	X				X			
Print files/documents related to school work/learning		X						X
Print personal files/documents etc.				X	X			
Download and install unauthorised software on school devices	X				X			

Appendix 2: Acceptable Use Parental Agreement

Parents are requested to support the Acceptable Use statements identified in Appendix 1 where they apply to their children. The following statements outline this request. Parents will not be asked to sign this agreement, but will be made aware of the expectations on our website and in the Parent Handbook. Please also see Section 7 of the Online Safety Policy.

By sending their child to our school, parents also agree to the following statements:

- I will support the school in keeping my child safe when using the school's IT systems and internet. I understand the conditions set out in Appendix 1 of the Online Safety Policy for pupils using the school's IT systems and internet and will ensure my child also understands them.
- I will not post material online that may bring the school or any individual within it into disrepute. (Rather than posting negative material online, any parent concerned about an aspect of school should contact a member of staff and share their concern. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).
- I will only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.
- I understand that under no circumstance should images be taken at any time on school premises or events of anyone other than my own child/ren, and that I will not post anywhere online or otherwise publish images that contain anyone other than my own child/ren.

Support for Parents

Please speak to your child's class teacher if you have any concerns about your child's online safety. You can also speak to or email our Safeguarding Leaders – safeguarding@allsaints.herts.sch.uk

Parents can also find resources to support them in keeping their children safe at home through the following websites:

- NSPCC: Online Safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

- NSPCC: Social Media: https://www.nspcc.org.uk/keeping-children-safe/online-safety/social-media/

- Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/parents-and-carers

- Government Guidance: https://www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online/coronavirus-covid-19-support-for-parents-and-carers-to-keep-children-safe-online

- 2 Johns Online Safety: https://esafetytraining.org/resources/parents-carers-area/

Thank you for your support and assistance in keeping our school community safe.

Appendix 3: Acceptable Use Agreement for staff, governors, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Sign up to online services, subscriptions, or other systems for use in or for school (including social media, blogs or sharing platforms) without specific permission from the headteacher
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community, including on personal social networks, systems and platforms
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I will report any breaches of the online policy, or any issues, problems, or concerns - whether accidental, suspected, or deliberate - to the headteacher and/or IT manager as soon as possible.

I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and IT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's IT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff/governor/volunteer/visitor):	**Date:**

Appendix 4: Guidance for staff on use of school IT systems and services

The school expects everyone to use internet, mobile and digital technologies responsibly and according to the conditions set out in the Online Safety Policy and the appendices. The policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff, governors, and volunteers (such as the PTA) should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Staff must not contact pupils, parents or conduct any school business using a personal email address.

Pupils should use school approved accounts on the school system for educational purposes. Where required, parent/carer permission will be obtained for the pupil account to exist.

For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Protection policy (GDPR). Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Personal devices used to access school email must have appropriate safeguards to prevent unauthorised access to school/work emails due to confidentiality – e.g. multi-factor authentication (MFA).

Users must not:

- open emails or attachments from suspect sources and should report their receipt to the Headteacher and IT Manager.
- send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites (including use of AI) and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required.
- If internet research is set for homework, specific sites will be suggested that have been checked by the teacher.
- All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or making use of other online content, such as Artificial Intelligence (AI) that may require sharing personally identifiable information about any member of the school community.
- Staff must not use personal accounts for online resources or outside activities that will include sharing of personally identifiable information about any member of the school community.
- When working with pupils, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

- Access or attempt to access any online material, website, app, blog, social media that may relate to illegal activity, or cause harm to individuals within the school community or harm the reputation of the school.
- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

School devices should be used to conduct school business outside of school. If using a personal device staff should use remote access to the school server to ensure that files are not saved locally to their own device. Staff must also ensure that no other user of that device (such as a shared family laptop) has access to school data or systems (such as login details etc.) at any time, and that the device is secured with a login password as a minimum.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by a member of the Senior Leadership Team.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See Data Protection policy (GDPR) for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the Headteacher in consultation with the IT Manager. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Images of staff are used for security purposes (ID cards and staff photo board), and as part of personnel records (the school's MIS system).

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Specific members of staff (usually SLT) are permitted to use their personal mobile phone to contact parents through the school telephone app.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Head Teacher or Deputy Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Designated areas are:

- Staff: the staff room, in classrooms only when no children are on site (not during the school day without explicit permission from the headteacher for specific, limited reason).
- Parents: the school car park, the playground (collection times only), the main entrance. If needed in a meeting room, permission should be sought from the member of staff leading the meeting (and children must not be present).

Year 5 and 6 pupils are allowed to bring personal mobile devices/phones to school but must turn them off upon arrival (at the playground gate) and hand them to the class teacher. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

If a pupil is suspected of doing so, the behaviour policy must be followed and the incident reported to a senior leader.

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles used to access school emails and data must have two levels of security set up to access information.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with Alison Brooks before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the headteacher or DDSLs. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.