St Ann's Heath Junior School

Online Safety Policy

This school is committed to safeguarding, child protection and promoting the welfare of children and young people and expects all members of the school and its community to demonstrably share this commitment. We aim to foster good relations between all members of the school community ensuring they are treated equally and without prejudice.

1. Aims……..Page 2
2. Legislation and guidance ……..Page 2
3. Roles and Responsibilities …….. Page 3
4. Educating children about online safety …….. Page 6
5. Educating parents / carers about online safety …….. Page 7
6. Cyber – bullying ……..Page 7
7. Examining electronic devices ……..Page 8
8. Use of social media ……..Page 9
9. Acceptable use of the internet in school ……..Page 10
10. Pupils using mobile devices in school ……..Page 10
11. Staff using work devices outside school ……..Page 10
12. How the school will respond to issues of misuse …….. Page 10
13. Filtering and Monitoring …….. Page 11
14. Online Publishing …….. Page 12
15. Data Protection …….. Page 12
16. Training …….. Page 13
17. Monitoring and Reviewing …….. Page 14

1. Aims

This Online Safety Policy outlines the commitment of St Ann's Heath Junior School to safeguard members of our school community online in accordance with statutory guidance and best practice.

It applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

St Ann's Heath 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.

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

3. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Co-Head Teachers and Senior Leaders

- The Co-Head teachers (who are also the lead DSLs in school) have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Co-Head teachers are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (appendix 1).
- The Co-Head teachers are responsible for ensuring that all Designated Safeguarding Leads, IT provider/IT technician, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Co-Head teachers will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Co-Head teachers will receive regular monitoring reports/logs from the IT technician and these will be shared within safeguarding meetings as and when the need arises.
- The Co-Head teachers will work with the safeguarding governor, Deputy DSLs and IT service provider in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Safeguarding governor for the Governing Body. The Governing Body will receive regular information about online safety incidents and monitoring reports. The safeguarding governor will ensure there are:

- regular meetings with the Designated Safeguarding Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safeguarding Leads (DSLs)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- have a leading role in establishing and reviewing the school online safety policy
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- liaise with staff and IT provider on matters of safety and safeguarding and welfare (including online and digital safety)
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leader to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents (see appendix 3)
- provide training and advice for staff/governors/children /parents/carers

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA) (appendix 4)
- they immediately report any suspected misuse or problem to the DSLs for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use.
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider (Turn IT On)

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSLs for investigation and action
- the filtering is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Children

- are responsible for using the school digital technology systems in accordance with the children's acceptable use agreement (appendix 3) and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the children/parent acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.

- parents' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices when they are in the school

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and will be expected to read and follow it. If appropriate, they will be expected to agree to and sign the terms on acceptable use (appendix 4).

4. Educating children about online safety

Pupils will be taught about online safety as part of the curriculum. The school uses the Project Evolve resources based on the UKCIS framework 'Education for a Connected World' that covers knowledge, skills, behaviours and attitudes across eight strands of online safety. Online safety is taught at the beginning of every computing lesson to ensure that the online safety messages are covered regularly throughout the year.

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 Key stage at St Ann's Heath**, 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. Our curriculum incorporates and makes use of relevant national initiatives and such as Safer Internet Day and Anti-bullying week. 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/carers about online safety

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

The school will inform parents:

- What systems the school uses to filter and monitor online use
- What their children will be learning about during Computing lessons and the eight strands of online safety

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSLs/Co-Head Teachers.

Concerns or queries about this policy can be raised with any member of staff or the Co-Head Teachers.

6. Cyber-bullying

Definition

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

Preventing and addressing cyber-bullying

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

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

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

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

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour and Relationship 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.

7. Examining electronic devices

The Co-Head Teachers, and any member of staff authorised to do so by the Co-Head Teachers, 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, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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 the staff member in conjunction with the DSL and Co-Head Teachers 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.

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 DSLs 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
- The school's Behaviour and Relationship policy

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

8. Use of social media

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of the school community.

The term social media may include (but is not limited to) blogs, social and networking sites, forums, online gaming, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.

All members of the school community are expected to engage in social media in a positive and responsible manner.

All members of the school community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

Staff use of social media

The safe and responsible use of any social media sites will be discussed with all members of staff, including volunteers, as part of our staff code of conduct and Child Protection and Safeguarding policy and procedures.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with school policies.

Information and content that staff members have access to as part of their employment, including photos and personal information about children and their family members or colleagues will not be shared or discussed on social media sites.

Communicating with children and parents and carers

Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.

All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites or profiles.

Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the Co-Head Teachers. Decisions made and advice provided in these situations will be formally recorded in order to safeguard children, the member of staff and the setting.

Children's use of social media

St Ann's Heath will empower children to acquire the knowledge and skills needed to use social media in a safe, considered and respectful way and develop their resilience so they can manage and respond to online risks and know to share any concerns with a trusted adult. Safe and appropriate use of social media will be taught to all children as part of an embedded and progressive safeguarding education approach using age appropriate sites and resources.

Any concerns regarding children's use of social media will be dealt with in accordance with existing policies, including the Behaviour and Relationship policy and the Child Protection and Safeguarding policy.

Sanctions and/or support will be implemented and offered to children as appropriate, in line with our Child Protection and Safeguarding policy. Civil or legal action may be taken if necessary.

Concerns regarding children's use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

9. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 3 and 4). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements (AUA) in appendices 3 and 4.

10. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- School hours
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour and Relationship policy, which may result in the confiscation of their device.

11. Staff using work devices outside school

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

- Keeping the device password-protected
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring anti-virus and anti-spyware software are in place
- 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 appendix 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 Co-Head teachers.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

13. Filtering & Monitoring

The school filtering and monitoring provision is agreed by the Co-Head teachers, governors and the IT Service Provider and is regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems involve the specialist knowledge of both the DSLs and IT technician. At St Ann's Heath, the DSLs have the lead responsibility for safeguarding and online safety and the IT service provider has the technical responsibility.

Checks on the filtering and monitoring systems are carried out by the school's IT Service Provider with the involvement of the Co-Head teachers, the Designated Safeguarding Leads and a governor, in particular when a safeguarding risk is identified, there is a change in working practice if required.

Filtering

The school has filtering systems in place to protect the school, systems and users:

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the filtering provider RM by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a process in place to deal with, and log, requests/approvals for filtering changes.
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has provided user-based filtering
- access to content through non-browser services (e.g. apps) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SEGfL site - https://reportharmfulcontent.com/report/?from=button

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- the school monitors all network use across its devices and services.
- the school uses the software programme SENSO to monitor Windows devices.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- there are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies. These include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to DSLs/ Co-Head teachers
- pro-active alerts from SENSO inform the school of breaches, allowing effective intervention
- IT technician regularly reviews the activity of users on the school network

14. Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Newsletters and weekly Bulletins

The school website is hosted by e4education. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where children's work, images or videos are published, their identities are protected, and full names are not published.

15. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a General Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Retention Schedule' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the 'Retention Schedule' lists the lawful basis for processing personal data (including, where relevant, consent).
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'Retention Schedule" supports this.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data

- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law.

16. Training

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

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and CPD meetings). Staff are also required to complete a self-audit annually to assess online safety training needs (see appendix 5).

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

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

Volunteers will receive appropriate training and updates.

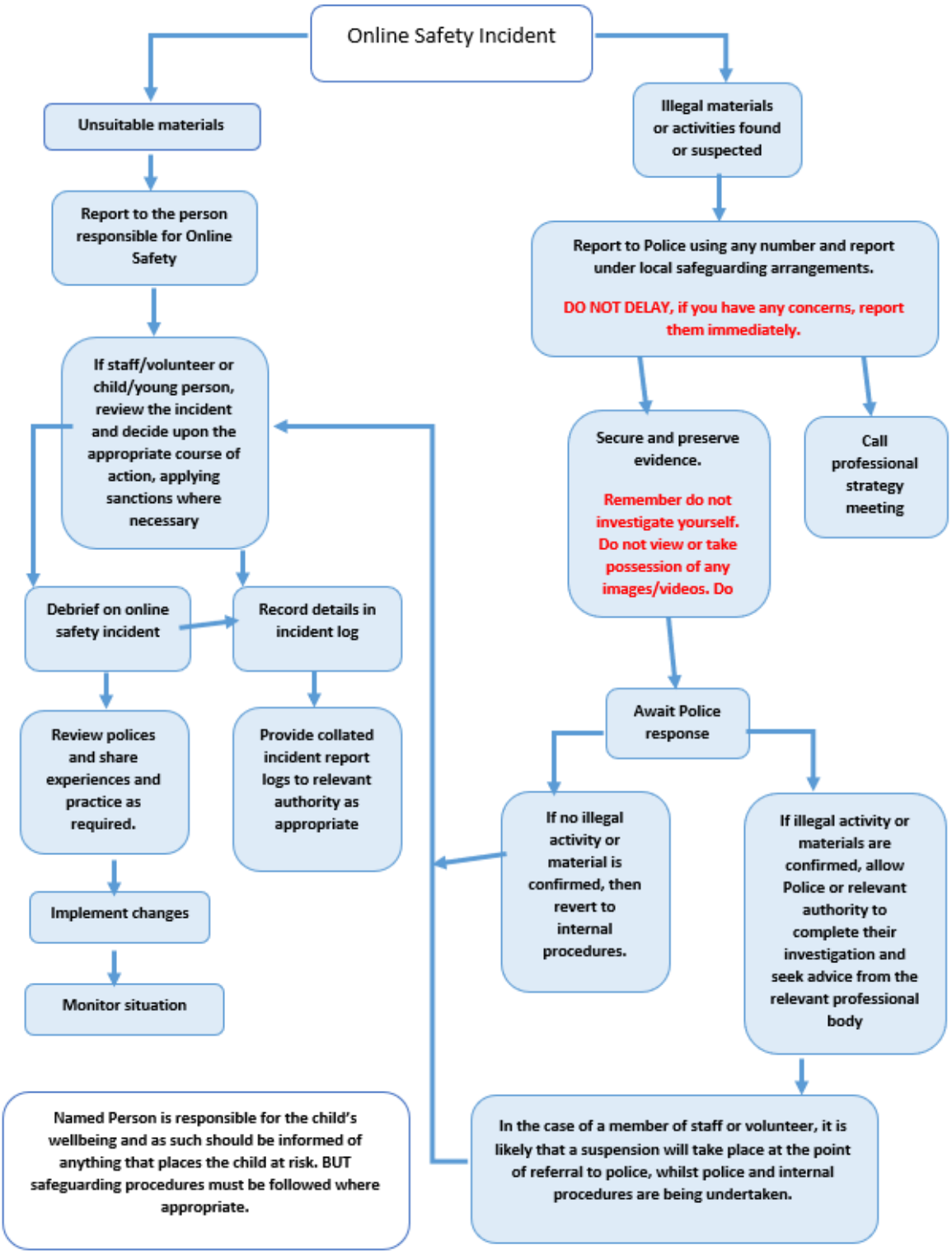
More information about safeguarding training is set out in the school's Safeguarding and Child Protection policy.

17. Monitoring and Reviewing

The implementation of this policy is monitored by the Co-Head teachers and SLT and by Governors to evaluate its implementation and effectiveness. This policy will be reviewed every year, or earlier if the need arises. This policy will be promoted and implemented throughout the school.

Policy Status	
Agreed by Governors	September 2024
Agreed by Staff	September 2024
Next Review Date	September 2025

Appendix 1 – Online Safety Incident Flowchart



Appendix 2 – Online Safety Incident form for reporting online safety concerns

	St Ann's Heath Junior School
	Online Safety Incident form
	Any member of the St Ann's Heath school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the concern. It is important that you provide as much detail as possible. Once completed please hand this report to Jackie King/Pip O'Connor (DSLs) or Sian Savill/Laura Allen (DDSLs).

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, transphobic, bi-phobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Online radicalisation	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.
Action taken	Specify any action taken i.e. removal of equipment, spoken to parents/carers, sought advice form DSL etc, reported police, reported to IT
Outcome of incident	

Appendix 3: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement.

When I use the school's ICT systems (computer/iPad) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or responsible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone into school:

- I will ensure that my mobile device is turned off when entering the school site and handed in to a member of staff at the start of the school day. I will be responsible for collecting it and will ensure that it is not switched on until I have left the school site
- I will not use my mobile device during lessons, clubs or other activities organised by the school
- I am aware that the school cannot be held responsible for the loss or damage of my mobile phone
- I will use my mobile device responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal mobile phones in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement (staff, governors, volunteers and visitors)

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

Name of staff member/governor/volunteer/visitor:

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
- 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 Senior Leadership Team first
- Share confidential information about the school, its pupils or staff, or other members of the community
- 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

If I bring a personal mobile phone into school:

- I will ensure that my mobile device is not on my person in and around school whilst in the presence of children
- I will not use my mobile device to take photos of children unless authorised to do so by a member of the SLT

I will only use the school's ICT 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 am aware that the school has filtering and monitoring systems in place when I am using the school's ICT facilities.

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 Leads (DSL) 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 ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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

Appendix 5: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person (s) who has/have lead responsibility for online safety in school?	
Are you aware of the different ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue linked to online safety?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	