Abbey Hill Primary and Nursery School

Online Safety Policy

Adopted by the Governing Body: 4th October 2022

Next Review: October 2024

Abbey Hill Primary and Nursery School Online Safety Policy

Key Roles and Responsibilities

Designated Safeguarding Leads: Ms H Chambers and Ms S Jeffs

Online Safety Lead:

Online Safety Link Governor: Mr K Simpson

Network Manager: Mr C Savage (Infotech)

Overview

Our children grow up in an increasingly complex world, living their lives on and off line. This presents many positive and exciting opportunities, as well as challenges and risks. The use of the latest technology is actively encouraged at Abbey Hill but with this comes a responsibility to protect both pupils and the school from abuse of the system.

Online safety is an integral part of safeguarding and this policy is written in line with Keeping Children Safe in Education 2022 (KCSIE) and other statutory documents. It is designed to sit alongside the school's Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

Aims

This policy aims to:

- Set out expectations for all members of the Abbey Hill community when using digital technology.
- Help all stakeholders to recognise that standards for online and digital behaviour, including social media activity, apply beyond the confines of the school gates and school day, regardless of device or platform
- Promote the safe, responsible and respectful use of technology to engage children in their learning, to improve attainment, and to prepare children for the opportunities and risks of the digital world, to enable them to survive and thrive online
- Help school staff understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children in their care
    - for their own protection, minimising misplaced or malicious allegations
    - to understand their own standards and practice
    - to support the school's ethos, aims and objectives and protect its reputation in the wider community
- Establish clear procedures for managing any online incidents.

This policy applies to all members of the Abbey Hill community including staff, pupils, parents and carers, governors, volunteers, visitors and contractors who have access to our digital technology, networks and systems, whether on-site or remotely at any time.

Roles and Responsibilities

Our school is a community and all members have a duty to behave respectfully and to report immediately any concerns or inappropriate behaviour online or offline in order to protect staff, pupils,

families and the reputation of the school. We learn together, make honest mistakes together and support each other in both the online and offline world.

Head teacher Responsibilities

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the DSL team and ensure that DSL responsibilities listed in the section below are being followed and fully supported (at Abbey Hill the head teacher is also a DSL).
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and guidance from Nottinghamshire Children's Safeguarding Partnership (NSCP).
- Liaise with the DSL team and the online safety lead on all online safety issues and receive regular updates on local and national guidance.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling.
- Work with the DSL team and school business manager to ensure a GDPR compliant framework for storing data, ensuring child protection is always put first and data protection processes support the legal sharing of information.
- Ensure the school makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised.
- Ensure the governing body is regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Team and Online Safety Lead Responsibilities

The DSL team will take lead responsibility for Child Protection and Safeguarding including online safety.

The Online Safety Lead will work alongside the Deputy DSL to ensure an effective approach within the school.

The Online Safety Lead and the Deputy DSL will meet on a regular basis.

- Liaise with the Local Authority TETC team and work with other agencies in line with Working Together to Safeguard Children.
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the headteacher and school business manager to ensure a GDPR compliant framework for storing data, ensuring child protection is always put first and data protection processes support the legal sharing of information.
- Stay up to date with the latest trends in online safety.
- Receive regular updates in online safety issues and legislation and be aware of local and national trends.

- Ensure online safety education is embedded across the curriculum and in the wider life of the school.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents including hard-to-reach parents.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with the senior leadership team and safeguarding governor to discuss current issues, review incident logs and discuss filtering and monitoring.
- Ensure all staff are aware of the procedures to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss appropriate filtering and monitoring with the technical support manager and ensure staff are aware.
- Ensure the 2022 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to cyber-bullying.
- Facilitate training and advice for all staff on KCSIE Part 1 and Annexes A and C

Whole Staff Responsibilities

- Understand that online safety is a core part of safeguarding and as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Lead and Online Safety Lead are.
- Read Part 1, Annex A and Annex B of Keeping Children Safe in Education 2022.
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy.
- Report and record online-safety incidents in the same way as safeguarding incidents.
- Sign and follow the Staff Code of Conduct.
- Notify a member of the DSL team if policy does not reflect practice in our school and follow escalation procedures if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities, both in the curriculum and outside the classroom, making the most of unexpected learning opportunities as they arise.
- Monitor what pupils are doing and consider potential dangers and the age appropriateness of websites whenever teaching online lessons. Encourage sensible use by pupils at all times.
- Supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking e.g. challenging fake news, age appropriate materials and data law. Ensure lessons cover how to keep personal information private, and help pupils navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Explain and discuss the pupil acceptable use policy, refer to it regularly in lessons and whenever an incident arises.
- Notify the DSL team of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual harassment online.
- Be aware that you are often most likely to see or overhear online-safety issues, particularly relating to bullying and sexual harassment and violence in the playground, corridors and other communal areas outside the classroom – always inform the DSL team.
- Receive regular updates from the DSL and maintain a professional curiosity for online safety issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside school hours and off the school site, and on social media, in all aspects upholding the reputation of the school and all staff.

- Follow the remote learning policy and teacher protocols during any part or full school closure.

Governor Responsibilities

- Understand that online safety is a core part of safeguarding and as such it is part of everyone's job in our school.
- Know who the Designated Safeguarding Leads (DSL) and Online Safety Coordinator (OSC) are.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education 2022.
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy.
- Notify a member of the DSL team if policy does not reflect practice in our school and follow escalation procedures if concerns are not promptly acted upon.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and the governing body.

PHSE Lead Responsibilities

As listed in whole staff responsibilities plus:

- Embed consent, mental well-being, healthy relationships and staying safe online in the PSHE and Relationships Education curriculum, and how to use technology safely, responsibly and respectfully. Ensure lessons cover how to keep personal information private, and help pupils navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the DSL team and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and Relationships Education.

Computing Curriculum Lead Responsibilities

As listed in whole staff responsibilities plus:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the National Curriculum.
- Work closely with the DSL team and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with the acceptable use policy, including any arrangements for remote learning.

Network Manager Responsibilities

As listed in whole staff responsibilities plus:

- Keep up to date with the school's online safety policy in order to carry out their online safety role effectively and to inform and update others.
- Work closely with the DSL team and online safety lead to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand existing services and any changes to these systems especially in terms of access to personal and sensitive records, to data and to systems such as access to YouTube, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of appropriate filtering and monitoring as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures.
- Report any online-safety related issues that come to their attention in line with school policy.

- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology, online platforms and social media presence and ensure any misuse or attempted misuse is identified and reported in line with school policy.

Pupil Responsibilities

- Read, understand, sign and keep to the pupil acceptable use policy.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school, and realise that the school's acceptable use and remote learning policies cover actions out of school, including on social media.
- Understand the benefits and opportunities and the risks and dangers of the online world and know who to talk to at school or outside school if there are problems.

Volunteer, Visitor and Contractor Responsibilities

- Read, understand and adhere to the acceptable use policy.
- Report any concerns, no matter how small, to the Designated Safeguarding Lead or online safety led as named in this policy.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

Parent and Carer Responsibilities

- Read the pupil acceptable use policy and encourage their children to follow it.
- Inform school if they have any concerns about their children's use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media. Refrain from sharing images or details of others without permission and from posting negative, threatening or violent comments about others, including school staff, volunteers, pupils or other parents and carers.

Curriculum

The following subjects have the clearest online safety links:

- PSHE, Relationships Education and Citizenship
- Computing

At Abbey Hill we recognise that online safety and wider digital resilience must be a thread throughout the curriculum.

Curriculum plans and schemes of work, including for SEND pupils, are used as an opportunity to focus on the key areas of self-image and identity, online relationships, online bullying, managing online information and online privacy.

We follow a curriculum framework based on the National Curriculum which helps to equip children for life in a digital world. Online safety themes are also integrated regularly into our assemblies.

Handling Concerns and Incidents

It is crucial that all staff recognise online safety is a part of safeguarding, as well as being a curriculum strand of Computing, PSHE and Citizenship. Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom particularly relating to bullying and sexual harassment and violence.

Concerns must be handled in the same way as any other safeguarding concern; staff should speak to the DSL team or the online safety lead if something is of concern to them and record it on our CPOMs electronic safeguarding system.

We will take all reasonable precautions to ensure online safety, but recognise that incidents will occur both inside school and outside school, and that those from outside school will continue to impact on pupils when they come into school. All members of staff are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's safeguarding procedures.

Any suspected online risk or incident should be reported to the DSL on the same day – where urgent, it will be made immediately.

Any concern or allegation about staff misuse should be referred directly to the head teacher, unless the concern is about the head teacher in which case the complaint should be referred to the chair of governors and the LADO, Local Authority Designated Officer. Staff may also use the NSPCC Whistleblowing Helpline.

The school will also seek support from other agencies as needed e.g. the Local Authority, NSCP, Notts Prevent Officer, Police). We will inform parents and carers of online safety incidents involving their children and, where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law, the police.

System Security

- All computers and laptops are password protected. Passwords are changed on a regular basis.
- Staff and pupils should not make deliberate attempts to disrupt or damage the school network, any device attached to it or any data stored on it or transmitted across.
- Staff should not alter school hardware in any way.
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data.

Monitoring

The school reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused or that the terms of this policy are being breached, appropriate disciplinary action will be taken.

Property

Staff and pupils should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to the school's business manager.

Viruses

Staff and pupils should be aware of the potential damage that can be caused by computer viruses. They **must not** download, install or run any programs or data including computer games or open emails from unknown or unidentifiable sources.

The Internet

The School recognises the benefits of using the internet, as well as its risks and challenges. The internet facility is provided for school related activities only. The school internet system has a filtering and monitoring system run by FortiNet and Managed Engine, which monitor and filter all website access. Any inappropriate material, whether it be sexual, violent, extremist or illegal in nature will be blocked and the System Administrator alerted, who will in turn alert the DSL team and the online safety lead.

Viewing, retrieving or downloading any material that the school considers inappropriate will result in appropriate disciplinary action.

Personal Safety and Responsibilities for Staff, Pupils and Parents

Staff

It is crucial that staff are careful about content they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages.

Staff **must** ensure that films or other material shown to children are age appropriate.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher.

Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school uniform.
- Staff must not form online friendships with pupils and parents.
- Staff will be required to attend an annual safeguarding training, including online safety.
- Staff should use their school email account for all school-related communications.
- Staff members should refer to the Staff Code of Conduct for more detailed information.

Pupils

- The school will deliver internet safety lessons regularly. Pupils will be taught how to stay safe when working online at school and at home.
- Pupils should not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Pupils should never reveal their full name, address or contact details, any school or network user ID or password online, even to friends or family.
- Pupils should be aware that people online may not be who they say they are and can easily pose as someone else.
- Pupils should employ a healthy mistrust of anyone that they "meet" online unless their identity can be verified.
- Pupils will be taught they must never arrange to meet anyone you have met on the internet - people are not always who they say they are.
- The use of chat rooms and social networking sites are not permitted in school.

Parents

- Parents will be invited to an annual e-safety event run by the school's Network Manager consisting of advice and useful tips to help support them in ensuring their child's safety online.
- Parents will be informed about parental control software available to manage and control their child's internet activity and parental control software services to limit the kind of content children can access through their mobile phones.
- Parents must be aware that parental control software doesn't replace the need for supervision and education when working on the internet.
- We will encourage parents to take an interest in their children's internet use and discuss safety issues relating to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends" and remind them only to talk to people they know, never to give out any personal details or details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware they are in control and they have every right to check on their children's online activities as well as their mobile phone usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

If your child behaves inappropriately online

- Before doing anything, take a deep breath and remain calm. There's lots of information and advice on the http://www.thinkyouknow.co.uk site to keep your child safe and access support.
- Have a calm and open conversation with your child to explore what is happening in an honest and supportive way.
- Discuss your concerns with someone you trust e.g. a friend, partner or the school.
- Talk to a professional at the NSPCC helpline on 0808 800 5000 to help you decide the best action to take to ensure your child is safe.

Making a report about something online:

- For concerns about online grooming or sexual behaviour online contact CEOP on http://www.ceop.police.uk or click on the 'Report Abuse' button at http://www.thinkyouknow.co.uk.
- For criminal sexual or obscene content on the internet report to the Internet Watch Foundation: http://www.iwf.org.uk.
- Report directly to your local police force.
- For a child in immediate danger, call 999.

Parents can find out more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to children about e-safety at:

- The UK Safer Internet Centre website http://www.saferinternet.org.uk
- CEOP's Thinkuknow website http://www.thinkuknow.co.uk and http://www.thinkyouknow.co.uk/parents
- Internet Matters http://www.internetmatters.org

- Childnet http://www.childnet.com/sns
- NSPCC http://www.nspcc.org.uk/onlinesafety
- Parent Zone http://www.parentzone.org.uk
- Ask About Games (where families make sense of video games http://www.askaboutgames.com

Use of School Email

Personal use

Email is provided for school related purposes only. The school monitors the use of email and disciplinary action may be taken if inappropriate uses of personal emails are discovered.

Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. Pupils and staff should not include anything in an email that is not appropriate to be published generally. Any email message which is abusive, discriminatory on grounds of sex, race, disability, sexual orientation or religious belief, or defamatory is not permitted.

Privacy

All files and emails on the system are property of the school. As such, system administrators and staff have the right to access them if required

Secure Documents
All emails of a sensitive or secure nature should be sent using the phrase "secure message". The system will then automatically encrypt the message and any attachments. This uses several strong encryption protocols, and technologies that include Transport Layer Security, Secure Socket Layer (TLS and SSL), Internet Protocol Security (IPSEC), and Advanced Encryption Standard (AES).

Mobile Phones

Staff

- The school accepts that employees will bring their mobile phones to work.
- Mobile phones and personally owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
    - Employees are not permitted to make or receive calls or texts during lessons or formal school time or use recording equipment on their mobile phones or personal devices to take photographs or videos of children.
    - Staff use of mobile phones during the school day will normally be limited to the morning, lunch and afternoon break and after school.
    - Mobile phones should be switched off (or on silent) and left in a safe place during lesson times.
    - Staff should use phones in designated areas – the staff room or the school office. If a private call needs to be made then a request for a room can be made to the head teacher.
- Mobile phones are **not** permitted in areas where children are present unless a school phone is being used for a medical reason or the teacher is in a remote location e.g. the Pod, or on a class trip. Where there are insufficient school phones, staff members will be permitted to take their own phones on school trips for the purpose of keeping in touch when the whole class is not together. The trip leader will monitor the appropriate use of phones.

- If an employee has a particular reason for a specified period of time, they may request via the head teacher that they leave their phone on during working hours.
- Staff should ensure that their phones are protected with PIN or access codes in case of loss or theft.
- If a staff member breaches the school policy then disciplinary action may be taken as appropriate.

Pupils

The following rules apply for the use of personal mobile phones;

- Pupils are not permitted to bring mobile phones, smartwatches or personally owned devices into school.
- Pupils in KS2 who walk to and from school must hand in their mobile phones at the school office when they arrive in the morning for safekeeping in a locked location during school hours.
- Pupils must collect their mobile at the end of the day just before leaving the school premises.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers when they are able to collect them.

Acceptable Use of IT Policies

Child friendly policies for Key Stage One and Key Stage Two are attached to this policy in Annex 1. They will be displayed in classrooms and on the school's website, and sent home for parents to share with their children. Staff will ensure children understand the policies and refer to them in lessons and whenever incidents arise.