HEDGEWOOD SCHOOL

Online Safety Policy

2021 - 2022

September 2021

AUTISM
ACCREDITATION

HEDGEWOOD PRIMARY SPECIAL SCHOOL

Accredited by Elklan, AptEd and Afasic as
Communication
Friendly

ONLINE SAFETY POLICY

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach, and collaboration between school leads, all staff, pupils, and parents. This policy sits alongside our Child Protection and Safeguarding, Sex and Relationships, and Behaviour Policies. It is written in line with Keeping Children Safe in Education 2021 (KCSIE), Teaching Online Safety in Schools 2019, and statutory Relationships Education and Health Education guidance 2019. It is essential that children are safeguarded from potentially harmful and inappropriate online material. We aim to have an effective whole school approach to online safety that empowers our school to protect and educate pupils, staff, and parents in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. It is a safeguarding priority as our pupils are known to be more vulnerable online.

Introduction

Children use the internet in educational, creative, empowering and fun ways. However, children with SEN are more vulnerable to online safety risks. For example:

- Children with Autism will make literal interpretations of content which will affect how they respond and correspondingly more vulnerable.
- Children with complex needs do not always understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.
- Some children with SEN may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.
- They may not appreciate how their own online behaviour may be seen by someone else as bullying.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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.

These four areas are a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all four.

In past and potential future remote learning and lockdowns, there is greater risk as children spend more time at home and on devices.

Roles and Responsibilities

All members of the Hedgewood school community have a duty to safeguard children, behave respectfully online and offline, and immediately report any concerns or inappropriate behaviour.

The Senior Leadership Team
Key responsibilities:

- Promote a culture of safeguarding where online safety is fully integrated into whole school safeguarding.
- Regularly ensure that policies and procedures are followed by all staff
- Ensure that this aspect of safeguarding is covered in staff induction
- Undertake training in online safety, alongside safeguarding training.
- Liaise with the Designated Safeguarding Lead (DSL) on all online safety issues.
- Ensure that the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring and protected email systems.
- Ensure governors are regularly updated on the nature and effectiveness of our school's arrangements for online safety.
- Understand the procedures to be followed in the event of a serious online safeguarding incident.
- Work closely with RSHE and Computing leads to avoid overlap but ensure a complementary whole school approach.

The Designated Safeguarding Lead (DSL)
Key responsibilities:

- Take lead responsibility for safeguarding and child protection, including online safety.
- Liaise with staff on matters of safety and safeguarding (including online safety) and when deciding whether to make a referral.
- Review remote learning procedures, rules and safeguards.
- Provide online safety training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins and staff meetings).

- Review and update this policy and other online safety documents.
- Work collaboratively with curriculum leads to ensure online safety education is embedded across the curriculum in line with the statutory RSHE and Teaching Online Safety in Schools guidance; this will be supported by use of the UK Council for Internet Safety framework ‘Education for a Connected World – 2020’ and Childnet STAR SEND toolkit to equip, enable and empower our teaching staff with the relevant knowledge they need to support our SEN pupils.
- Promote an awareness of and commitment to online safety throughout the school community.
- Raise parents’ awareness of online safety in workshops, communications home, and information via our school website.

All staff
Key responsibilities:

- Read and demonstrate their understanding of KCSIE 2021 and be aware of Annex D (online safety).
- Pay particular attention to our safeguarding provisions for home learning and remote teaching.
- Recognise that online safety is a part of safeguarding and a curriculum strand of RSHE and computing.
- Record online safety concerns in the same way as any safeguarding concern and report it in accordance with our school safeguarding procedure.
- Follow the staff acceptable use policy and staff code of conduct.
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with RSHE curriculum.
- Supervise pupils’ internet activity.
- In the event of a pupil being unintentionally exposed to undesirable materials, this must be logged with our ICT technician and reported to our senior leadership team immediately.

ICT Technician
Key responsibilities:

- Support and advise the DSL and senior leadership team on the implementation of appropriate filtering and monitoring.
- Use LGfL filtering software to block / filter potentially harmful and inappropriate content and contact online.
- Ensure that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Regular checks to ensure that our filtering methods are appropriate, effective and reasonable.

Parents / Carers
Are expected to:

- Promote positive online safety and model safe, responsible and respectful behaviours in their own use of technology.
- Consult with school if they have any concerns about their child and others’ use of technology
- Keep up-to-date with the risks / dangers of the online world and how to report online safeguarding incidents that happen at home

- Familiarise themselves with apps and websites that can provide further guidance on keeping children safe online e.g. LGfL Parent Safe, NSPCC Net Aware, and National Online Safety Mobile App.

Pupils
Will be encouraged to:

- Treat themselves and others with dignity and respect online
- Engage in online safety learning activities
- Speak to a trusted adult if they see something online that worries or upsets them

Governing Body
Key responsibilities:

- Approve this policy and subsequently review its effectiveness.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Ensure that appropriate monitoring systems and filters are in place and that children are taught about safeguarding, including online safety, with careful consideration of the range of special educational needs and disabilities of our pupils.

Education and Curriculum

Our pupils will be taught about online safety as part of the curriculum. It is incorporated into all our curriculum pathways (Essential for Living, Foundations for Life and Core Curriculum). When planning and delivering online safety, each pupil's autism and associated learning difficulties, communication needs, social interaction, independence and emotional well-being will be considered.

The following subjects have the clearest online safety links:

- RSHE
- Computing

However, it is the role of teaching staff to identify opportunities to thread online safety through all school activities, supporting curriculum leads and making the most of learning opportunities as they arise. Whenever overseeing the use of technology (iPads, laptops, internet) in schools, staff should carefully supervise and guide pupils, encourage safe use, monitor what pupils are doing and consider potential risks and age appropriateness of websites / apps.

At Hedgewood, we are working to adopt the early learning outcomes of the cross-curricular Internet Safety framework 'Education for a Connected World – 2020' alongside Childnet STAR SEND toolkit to equip, enable and empower our teaching staff with the relevant knowledge they need to support our SEN pupils. Staff will use their experience and knowledge to select and adapt activities from the toolkit to best suit the purpose of teaching our pupils in the four key areas:

- **S – Safe**: Be safe with what you share about yourself and others online
- **T – Trust:** Not everything or everyone is trustworthy online
- **A – Action:** Take positive action and always tell someone if anything worries or upsets you online
- **R – Respect:** Be kind online.

Remote Learning

Staff will maintain professional practice and adhere to our school protocols when communicating with parents (and pupils) remotely. This also includes our school protocols regarding staff conduct on social media. Staff will not agree to or suggest video calling pupils or families via apps that have not been agreed for use by the senior leadership team and will not share their personal contact details with parents/carers or pupils. Communication will remain within school hours as much as possible and only through school channels (e.g. Seesaw) and devices approved by the senior leadership team. On the rare occasion that staff need to use their personal mobile to call a parent / carer, they will ensure that they block their number from being displayed. Staff will be mindful of their surroundings during video calls. They will ensure that their background is clear from any private information or images.

Educating Parents About Online Safety

Hedgewood school will raise parents' / carers' awareness of internet safety in workshops, communications home, coffee afternoons, our website and social media page. If parents / carers have any queries or concerns in relation to online safety, these should be raised with the Designated Safeguarding Lead or a Deputy Designated Safeguarding Lead.

Handling Online Safety Concerns / Incidents

It is vital that all staff recognise that online safety is part of safeguarding. All concerns must be handled in the same way as any other safeguarding concern in line with our school's safeguarding policy and procedures and referred directly to the DSL. Hedgewood school commits to take all necessary precautions to ensure online safety, and recognise that incidents can occur both inside and outside school. All online safety concerns must be reported to the DSL, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors and the Local Authority's Designated Officer (LADO). We will actively seek support from other agencies as needed, e.g. the local authority multiagency safeguarding hub (MASH) and Prevent, NSPCC, LGfL, and National Crime Agency Child Exploitation and Online Protection (CEOP).

Hedgewood school uses an educational Internet Service Provider (ISP) with a filtering service that blocks access to sites which the filtering service recognises as unsuitable. However, no filtering service is fool proof and in the event of a pupil being unintentionally exposed to undesirable materials, the DSL and/or headteacher should be notified by the teacher / teaching assistant. The incident should be recorded by the DSL and the child's parent should be notified at the discretion of the DSL / headteacher according to the degree of seriousness of the incident.

Cyber-bullying

Cyber-bullying is bullying that takes place online, such as through social networking sites, messaging apps or gaming sites. It should be treated like any other form of bullying. Most of our pupils have an autism diagnosis with social interaction difficulties. This can lead to social misunderstanding and confusions. Our school's positive approach to behaviour shapes our ability to manage behaviour and empower our pupils to function appropriately at school, at home, in the community and online. Bullying and cyber-bullying are both forms of peer on peer abuse. Our aim is to create an atmosphere which is caring, protective and supportive where no one feels humiliated, intimidated or abused. Our Anti-Bullying Policy outlines the steps we take as a school to prevent and challenge bullying in all its forms.

Filtering and Monitoring

Hedgewood school is committed to ensure appropriate filters and appropriate monitoring systems are in place so that our pupils are not able to access harmful or inappropriate material. The appropriateness of any filters and monitoring systems will be informed in part, by the risk assessment required by the Prevent Duty.
Our internet connection is controlled by LGfL. This means that we have a dedicated, secure and safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen. WebScreen is made specifically to protect children in schools. We block / filter access to social networking sites using LGfL filtering software.

Acceptable Use of Internet in School

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 monitor the websites visited to ensure compliance. Further information is set out in our acceptable use policies.

Electronic communication

Hedgewood staff use the StaffMail system for all school emails. This system is linked to the Unified Sign-On (USO) authentication system and is fully auditable, trackable and managed by LGfL on behalf of the school. If sensitive data needs to be shared with external agencies. Egress systems are available for use.

Email, Seesaw and ParentMail are the official electronic communication channels between parents and the school.

Data protection

GDPR does not prevent, or limit, the sharing of information for the purpose of keeping children safe. Rigorous controls on the LGfL network, USO sign on, Sophos Anti-Virus, firewalls and filtering are all used to protect the integrity of data. All safeguarding data is highly sensitive and will be treated with the strictest confidentiality at all times. This data will only be shared via approved channels to colleagues or agencies with appropriate permissions.

Digital Images and Video

When a pupil joins Hedgewood, parents / carers are asked if they give consent for their child's image to be captured in photographs or videos and their consent for how their child's photograph will be used, e.g. displays, school website, Seesaw, school prospectus. Whenever a photograph or video is taken / made, staff will check the latest database before using it for any purpose.

Only school password protected and / or encrypted devices will be used to take photographs / videos of pupils and they will be stored on the school network in line with the retention schedule of the school Data Protection Policy. No member of staff, visitor or volunteer will use their personal phones or devices to capture photos or videos of pupils.

Personal Mobile Phones and Devices

Staff will ensure that personally owned mobile phones and devices will not be used in any way during lessons, clubs or formal school time, unless agreed by a member of the senior leadership team for a particular purpose with safeguards in place. Devices may be used by staff during their break times in the staff room. They must not be taken into vulnerable areas including the toilets and changing areas.

We do not allow pupils to have mobile phones or devices on school property. Should they be brought into school, they will be kept safe and handed to the parent (or passenger assistant if on SEND transport) at the end of the school day. If a pupil needs to bring in a personally owned device for a curriculum based activity or other specific need, this will need to be agreed by the headteacher with clear protocols in place for its use. Hedgewood school reserve the right to search the content of a pupil's personally owned device on school premises where there is reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

This policy should be read in conjunction with other school policies including: Child Protection and Safeguarding policy, Anti-bullying policy, ICT and Computing Policy, Code of Conduct policy

POLICY REVIEW DETAILS

Document Reviewed by SLT/GB annually or in response to changed government advice.

Readers are: staff, parents, governors, others

Adopted by GB in (date)