Online Safety Policy

Name of Subject Leader: Lauren Godfrey

Date policy formulated: November 2022

Date of review – November 2025

Development / Monitoring / Review of this Policy

This Online Safety policy was originally developed by a working group made up of:

- Headteacher & Senior Leaders
- Online Safety Officer / Subject Leader
- Staff – including Teachers, Support Staff, Technical staff
- Governors

This policy applies to all members of the Highfield Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the School.

Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 head teachers 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.

School Aims

- To have processes in place to ensure the online safety of pupils and staff.
- To 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 technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular

information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (Fiona Hodson). The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, alongside the supporting Online Safety Co-ordinator, Charlotte Morrissey.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This includes CPD, Online Safety Updates and Shadowing of colleagues.

Online Safety Co-ordinator/officer:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff

• receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

• meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting / committee of Governors

• reports regularly to Senior Leadership Team

Network Manager/Technical Staff:

The Network Manager / Co-ordinator for Computing is responsible for ensuring:

• that the school's technical infrastructure is secure and is not open to misuse or malicious attack

• that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.

• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

• the filtering policy), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

• that 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

• that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Online Safety Coordinator for investigation / action / sanction

• that monitoring software / systems are implemented and updated as agreed in school / policies

Parents

Parents are expected to:

• Notify a member of staff if they have any concerns or queries regarding this policy.

• Ensure their child has read, understood and agreed to the terms of the Pupil Acceptable Use policy.

Parents can seek further guidance on Keeping Children Safe online from the following organisations and website:

• UK Safer Internet Centre - https://saferinternet.org.uk/guide-and-resource/

• Childnet Advice - https://www.childnet.com/help-and-advice/parents-and-carers

• Child Exploitation and Online Protection - https://www.ceop.police.uk/Safety-Centre/

- Get Safe Online - https://www.getsafeonline.org/

Teaching and Support Staff:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices

- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction

- All digital communications with students / pupils / parents / carers should be 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

- Students / pupils understand and follow the Online Safety Policy and acceptable use policies

- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The three 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, anti-Semitism, radicalisation and extremism

- Contact – being subjected to harmful online interaction with other users, such as child-to-child 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.

Educating Pupils about online safety

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

- Understanding how to use technology safely, respectfully, responsibly, and securely.
- Recognising inappropriate content, contact, and conduct, and how to report concerns.
- Learning about online risks, including that any material someone provides to another, has the potential to be shared online. Also, the difficulty of removing potentially compromising material placed online.
- The impact of viewing, or sharing, harmful content.
- How to identify harmful behaviours online, and how to report it. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying 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 staff meetings). 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.

Handling Online Safety Complaints

- Complaints of internet misuse must be reported on CPOMS immediately for DSL to pick up.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding procedures.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues relating to online safety. This policy will be reviewed every three years.

At every review the policy will be shared with the school governors.

This policy should be read in conjunction with the Behaviour, Safeguarding and Code of Conduct policies.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Internal monitoring data for network activity
- Surveys / questionnaires of

o students / pupils

o parents / carers

o staff