Baldwins Hill Primary School

BALDWINS HILL SCHOOL

E-SAFETY POLICY

Review Date: April 2028

Agreed by Governors: April 2025

E-Safety Policy

Contents **Page**

Some guidance and wording adapted from "The Key for Leaders Model online safety Policy 2024"

E-safety Policy

The statutory curriculum requires children to learn how to locate, retrieve and exchange information using IT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed we must consider IT a life-skill.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Significant educational benefits result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

<u>Benefits of using the Internet in education include</u>:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- Educational and cultural exchanges between children world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for children and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- • Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfE.

<u>The 4 key areas of risk online that are addressed through our curriculum:</u>

- **Content** – Protecting children from illegal, inappropriate or harmful material, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism. Empowering children to know who they can ask if they see anything that makes them feel uncomfortable.
- **Contact** – Educating children on potential harmful online interaction with other users e.g. peer-to-peer pressure, inappropriate advertisements, adults posing as children or young adults.
- **Conduct** – Promoting responsible use of the internet and positive personal online behaviour to avoid causing harm/upset to others.
- **Commerce** – Protect children from risk such as online gambling, inappropriate advertising, phishing and/or financial scams

The school Internet access will be designed expressly for pupil use. Children will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access will be

planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age and stage of children.

Staff should guide children in on-line activities that will support the learning outcomes planned for the children' age and maturity. Children will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval. Unsuitable websites will be filtered; therefore inaccessible to staff and children. The use of Internet derived materials by staff and by children complies with copyright law. Children will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

E-mail

Email is an essential means of communication, and has significant educational benefits.

Children are taught how to use e-mail within our comprehensive scheme of learning, teaching them how to send emails within a safe environment where only the children and the teachers have access and all correspondences can be viewed and monitored where necessary. Children also have the ability to report any e-mail they deem inappropriate, sending the message directly to the class teacher.

Website management

The school website will be used to celebrate children's work, and to promote the Academy Trust.

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or children' home information will not be published.
- Website photographs that include children will be selected carefully and will not enable individual children to be identified.
- Children' full names will not be used anywhere on the website, particularly associated with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website.
- The ~~CEO and~~ Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Chat and instant messaging

- Children will not be allowed access to public or unregulated chat rooms.
- A risk assessment will be carried out before children are allowed to use a new technology in school.

Additional technology used for communications

Our policy is to discourage children from bringing mobile phones/smart watches to school. However, if parents wish their child to bring one for use before and after school, these must be handed in to the school office or class teacher where they will be stored in a teachers cupboard during school hours.

Smart Watches or similar devices that are able to send and receive messages or take photographs are prohibited in school. These items will be removed and returned to parents if brought into school.

Internet access

All classes are timetabled to learn about Computing which will include the use of laptops and other devices, and Micro:bit where necessary to the learning.

- The school will keep a record of all staff and children who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.

Risk assessments

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- All website access is filtered by SmoothWall Limited
- The Headteacher and the Computing Champion will ensure that the E-safety policy is implemented, and compliance with the policy monitored.

Filtering & Monitoring

- The school will work in partnership with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The Computing Lead will ensure that the filtering methods selected are appropriate, effective and reasonable.
- Smoothwall monitoring send the Headteacher/DSL reports of anything inappropriately typed or searched online

The school will monitor the impact of the policy using:

- *Cpoms logs of reported incidents*
- *Filtering and monitoring logs from Smoothwall acted on and monitored on arrival*

Children internet use

- Rules for Internet access will be posted near computer systems. (Page 5)
- Children will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Children will be taught E-safety lessons as part of the curriculum at the beginning of each half-term and children will be reminded of safe Internet use within these lessons.

In Key Stage (KS) 1, children will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Children in Key Stage (KS) 2 will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

By the end of primary school, children 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

- Internet Safety Day is always celebrated and a focus in school for all year groups.

Staff internet Use

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the school e-safety policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter.
- Staff development in safe and responsible Internet use, and on school E-safety policy will be provided as required.
- All staff accessing the school server or related websites remotely to ensure usernames, passwords and any other sensitive information is inaccessible to anyone else who may be using the device, such as personal laptop or iPad, and that they logout securely after each use.

Parents

Baldwins Hill will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website

The school will let parents/carers know:

What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Computing system security

Computing system security

- The school computing systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Memory sticks will not be used and where possible, files shared via cloud or email to be utilised instead.
- Unapproved system utilities and executable files will not be allowed in children' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

Complaints regarding internet use

- Prompt action will be required if a complaint is made.
- The severity of the incident will determine the course of action.
- Responsibility for handling incidents will be delegated to a senior member of staff.
- Parents and children will need to work in partnership with staff to resolve issues.
- Sanctions available include: Informing parents or carers, removal of internet or computer access for a period.

- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Any complaint about staff misuse must be referred to the Headteacher.

Google Classroom

'Where a pupil, class, group or small number of children need to self-isolate, or there is a local lockdown requiring children to remain at home, DfE expects schools to be able to immediately offer them access to remote education.' (www.gov.uk)

The purpose of our Google Classroom is to provide a safe and secure place to receive and share learning, and a place where we will be able to connect with school staff and classmates. In Google Classroom, school staff can assign work to the learners digitally, without paper. Google Classroom is accessible from any digital device with internet access and a web browser. Parents/carers can log in and view the assignments that their children have been set, whether their child has completed and submitted them, and view feedback that they may have received.

Early Years will continue to use Tapestry to share and submit their learning however, any live interactions will take place via Google Classroom.

Cyber-bullying

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 anti-bullying policy.)

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

Through the aforementioned curriculum, staff will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (see behaviour for learning policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or
Is identified in the school rules as a banned item for which a search can be carried out, and/or
Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above. (See behaviour for learning policy),

If inappropriate material is found on the device, it is up to Headteacher with the DSL, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) 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
- Our behaviour 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.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Baldwins Hill Primary recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Baldwins Hill Primary will treat any use of AI to bully pupils in line with our anti-bullying policy.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

Responsible Internet Use

We use the school computers and Internet connection for learning. These rules will help keep everyone safe.

- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will be **responsible** by only using my own network login and password.
- I will show **respect** by only looking at or deleting my own files.
- I must not bring software, memory cards, USB sticks or disks into school without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be **compassionate**: polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will have the **courage** to tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of E-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.