ONLINE SAFETY POLICY

Highfield Online Safety Policy 2022-23

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff 'in this policy) as well as pupils and parents/carers. All parties as outlined are collectively referred to as the 'school community'.
This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop, tablets, or mobile phones.
The Person responsible for overseeing all elements of online safety at Highfield Primary is Jonathan Feeley, Headteacher with the support of Linda Harrower, Computing and Online Safety Lead. Other school staff may also be involved with this e.g., safeguarding team.

ONLINE SAFETY POLICY

Policy Aims

The purpose of Highfield Primary School online safety policy is to:

- Safeguard and protect all members of Highfield Primary School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

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 fake news and self-image.
- **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.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as online bullying.
- **Commerce** – risks such as advertising, phishing and/or scams

It considers the DfE statutory guidance "Keeping Children Safe in Education" 2021.

Policy Scope

At Highfield Primary School we want to ensure that all members of our community are safe and responsible users of technology. We recognise the educational and social value of technology used in a responsible and positive way. We also recognise our responsibility to support young people and staff to manage risks when using technology.

Computing covers a wide range of resources, including web based and mobile learning. It is also important to recognise the constant and fast-paced evolution of technology within our society.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Microsoft Teams

- Mobile/ Smart phones with text, video and/ or web functionality
- Making /receiving phone calls via their mobile phones
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms such as Seesaw, TTRS, Tapestry
- Blogs and Wikis
- Music Downloading
- Online shopping (with adult's permission)

ONLINE SAFETY POLICY

This online safety policy recognises the commitment of our school to online safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology.

We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. This policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

Links with other policies and practices

This policy links with several other policies including:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Child Protection policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data Protection Policy
- Staff Disciplinary Policy

Monitoring and Review

Highfield Primary School will regularly review this policy and revise it in line with any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied. To ensure oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes. Any issues identified will be incorporated into the school's action planning.

Roles and Responsibilities

We believe that online safety is the responsibility of the whole school community.
The Senior Leadership Team will:

- Ensure liaison with the Governors about online safety
- Develop and promote an online safety culture within the school community
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements

- Ensure all members of school staff are aware of the contents of the school's Online Safety Policy and the use of any new technology within school
- Ensure all staff, pupils, occasional and external users of our school ICT equipment are issued with the relevant Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Ensure that Online safety is taught as part of the curriculum in an age-appropriate way to all pupils
- Make this Online Safety Policy available to all parents, carers and others via the school website

- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks
- Ensure technical support is in place to maintain a secure ICT system
- Receive and regularly review online safety incident log
- Ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required
- The Headteacher will take ultimate responsibility for the online safety of the school community

Responsibilities of the Headteacher, with the support of the Computing Leader:

- Promote an awareness and commitment to online safety throughout the school
- Take day to day responsibility for online safety within the school
- Liaise with technical staff on online safety issues
- Create and maintain online safety policies
- Develop an understanding of current online safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training on online safety issues
- Ensure that online safety is promoted to parents and carers
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- To promote the positive use of modern technologies and the Internet
- To ensure that the school online safety policy is reviewed

Responsibilities of all Staff:

- Read, understand, adhere to and help promote the school's online safety policies and guidance
- Take responsibility for the security of school systems and the data they use, or have access to
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school-based systems, NEVER through personal email, text, mobile phone, social network or other online medium
- Embed online safety messages in learning activities where appropriate

- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur to their line manager

Responsibilities of Technical Staff:

- Provide technical support and perspective to the Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures
- Implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Ensure appropriate filtering and monitoring systems are in place and that these are kept up to date
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Report any filtering breaches to the Senior Leadership Team, as well as, the school's Internet Service Provider or other services, as appropriate
- Ensure that provision exists for misuse detection and malicious attack
- Report any online safety-related issues that come to their attention to the online safety lead
- Ensure that procedures are in place for new starters and leavers to be correctly added to, and removed from, all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the school's ICT equipment
- Ensure appropriate back-up procedures exist, so that critical information and systems can be recovered in the event of a disaster
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Responsibilities of Pupils:

- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings and rights of other pupils
- Ensure they respect the values of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices

- To know, understand and follow school policies regarding bullying (including cyber-bullying)
- To support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

Responsibilities of Parents & Carers:

- Help and support the school in promoting online safety
- Read the school AUPs and encourage their children to adhere to them.

- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute
- To report concerns to the online safety lead
- To seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Contribute to the development of the school online safety policies
- Use school systems, such as learning platforms, and other network resources, and social media channels in a safe and appropriate way
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Responsibilities of the Governing Body:

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance, as part of the school's overarching Safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the Internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement their online safety strategy

Responsibilities of Child Protection Officers:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate
- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information
- Be aware of and understand the risks to young people from online activities, such as grooming for sexual exploitation, sexting, cyber bullying and others
-

- Raise awareness of the issues which may arise for vulnerable pupils in the school's approach to online safety, ensuring that staff know the correct child protection procedures to follow
- Respond appropriately to concerns raised by the monitoring systems in relation to safeguarding
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- Report online safety concerns, as appropriate, to the Senior Leadership Team and Governing Body

Educating Pupils about online safety

Online Safety education will be provided in the following ways:

- Key Online Safety messages can be reinforced as part of a planned programme of assemblies/pastoral activities
- Pupils should be taught in appropriate lessons to be critically aware of the materials / content they access online and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet, and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Online Safety guidance will be posted in the ICT suite

Staff should act as good role models in their use of ICT, the Internet and mobile devices

Highfield Primary School Online Safety Scheme of Work

Year Group	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Reception	Going Places Safely	A-B-C Searching	Keep It Private	My Creative Work	Sending Email	Review of themes taught throughout the year. Possible recap of lesson(s) if there is a need within the year group. Some lessons may be spilt over two half terms.
Year 1	Going Places Safely	A-B-C Searching	Keep It Private	My Creative Work	Sending Email	
Year 2	Staying Safe Online	Follow the Digital Trail	Screen Out the Mean	Using Keywords	Sites I Like	
Year 3	Powerful Passwords	My Online Community	Things for Sale	Show Respect Online	Writing Good Emails	

ONLINE SAFETY POLICY

Year 4	Rings of Responsibility 	Private and Personal Information 	The Power of Words 	The Key to Keywords 	Whose Is It, Anyway? 	
Year 5	Strong Passwords 	Digital Citizens Pledge 	You've Won a Prize! 	How to Cite a Site 	Picture Perfect 	
Year 6	Talking Safely Online 	Super Digital Citizen 	Privacy Rules 	What's Cyberbullying? 	Selling Stereotypes 	

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Awareness and engagement with parents and carers

Highfield Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parents' evenings and transition events
- Drawing their attention to the school online safety policy and expectations in newsletters, letters, and on our website

- Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.

Access to School Systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for regular visitors, governors, and temporary staff, who may be granted a temporary login. In addition, there is access to guest Wi-Fi which

may be granted to visitors. These are all covered by the relevant Acceptable Use Agreements. All users are provided with a login appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their login and passwords.
Access to personal, private, or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Passwords
We ensure that a secure and robust username and password convention exists for all system access (email, network access, etc.) We provide all staff with a unique, individually named user account and password for access to IT equipment, email, and information systems available within school. All pupils have a unique, individually named user account for access to IT equipment and information systems available within school. All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their login details. All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their login details. They must immediately report any suspicion or evidence that there has been a breach of security. The school maintains a log of all access by users and of their activities, while also using the system to track any online safety incidents.

Password Guidance
Passwords should be difficult to guess and must meet the following criteria:
- Minimum of 8 characters
- At least 1 number and special character (e.g. punctuation)
- Contain a mix of uppercase and lowercase characters
- Password must be changed when prompted
- You must not reuse an old password

Using the Internet
We provide the Internet to:
- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others examination boards and others

Using Email
Email is regarded as an essential means of communication. Communication by email between staff and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. Access to school email systems will always take place in accordance with Data Protection legislation and in line with other school policies. All email activity is recorded in line with data protection laws. The school can view these records in situations where this is called upon. The forwarding of any chain

messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider. Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email. School email addresses and other official contact details will not be used for setting up personal social media accounts. Members of the school community will immediately tell a designated member of the safeguarding team if they receive offensive communication, and this will be recorded in the school safeguarding files/records. It is the personal responsibility of the email account holder to keep their password secure.

Acceptable Use Policy
Please refer to the Acceptable Use Policy for more information.

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.) 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. 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, assemblies, and other subjects where appropriate. All staff receive training regarding online safety.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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 Designated Safeguarding Leads will consider whether the incident should be reported to the police based on the severity of the incident.

Examining electronic devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or ask a parent/carer to ensure it is deleted

- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also retain devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school but are not permitted to use them anywhere within the school grounds at any time. This includes during:

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

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device. All mobile devices must be surrendered to the class teacher upon arrival at school.

Publishing Content Online

School Website

The school maintains editorial responsibility for any school-initiated website or publishing online to ensure that the content is accurate, and the quality of presentation is maintained. The school maintains the integrity of the school website, by ensuring that responsibility for uploading material is always moderated and that passwords are protected. The point of contact on the website is the school address, e-mail, and telephone number. Parents have the option to opt out, so that pictures of individual pupils are not published on the website. Group photographs do not have student surnames attached.

Online Material Published Outside the School

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school. Material published by pupils, governors, and staff in a social

context which is considered to bring the school into disrepute or considered harmful to, or harassment of, another student or member of the school community will be considered a breach of school discipline and treated accordingly.

Using Images, Video & Sound

We recognise that many aspects of the curriculum can be enhanced using multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound. Digital images, video and sound recordings are only taken with the

permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. We ask all parents/carers and/or the pupils for consent to use the photographs and video of their children to be used (in publications and on websites). For their own protection, staff or other visitors to school are directed not to use a personal device (mobile phone, digital camera, or digital video recorder) to take photographs of pupils. We are happy for parents to take photographs at school events but will make them aware that they are for personal use only and if they have taken photographs of children other than their own, they should not be uploaded to social media sites and can be only used for their personal use.

Pupils' Personal Use of Social Media

The school is aware that many popular social media sites state that they are not for children under the age of 13, and as such school will reinforce this message. Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Pupils will be advised:

- To consider the risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests, and clubs
- To only approve and invite known friends on gaming platforms and to deny access to others by making profiles private/protected
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- How to block and report unwanted communications and report concerns both within school and externally

Using Other Technologies

As a school, we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and the risks from an online safety point of view. We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils. Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Training

All new staff members will receive online safety training as part of their induction. All staff members will receive regular reminders related to their own and pupils' online safety. More information about safeguarding training is set out in our Induction Policy.

Dealing with online safety Incidents

ONLINE SAFETY POLICY

In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the online safety Lead, Child Protection Officer, their line manager or the Headteacher, who will then respond in the most appropriate manner. Instances of cyberbullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim. Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's online safety Lead and technical support and appropriate advice sought, and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies,
procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that student data has been lost. School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with Complaints and Breaches of Conduct by Pupils

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the student will work in partnership with staff to resolve any issues that arise
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal);

- Accessing inappropriate or illegal content deliberately
- Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- Staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities would normally be unacceptable;

- Accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time

- Accessing non-educational websites (e.g., gaming or shopping websites) during lesson time
- Sharing a username and password with others or allowing another person to login using your account
- Accessing school ICT systems with someone else's username and password
- Deliberately opening, altering, deleting, or otherwise accessing files or data belonging to someone else

ONLINE SAFETY POLICY

Headteacher: Jonathan Feeley
Computing and Online Safety Lead: Linda Harrower
Chair of Governors: Oliver Thorne

Approved:

Governing Body Approval: Teaching, Learning and Pupil Support Committee 25.04.23

Signed: