HOMEFIELD PRIMARY SCHOOL & SSC
Aiming high together

Online Safety and Acceptable Use Policy (Non Statutory)

Reviewer: Diane South/Barby Huntingford
Reviewed and approved by Full Governors:
Adopted by Governors on: 10/09/2024
Next Update: September 2027

HOMEFIELD PRIMARY AND SSC – ONLINE SAFETY AND ACCEPTABLE USE POLICY

AIMS

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

Roles and responsibilities

The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet.

The Head Teacher

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the, IT manager/co-ordinator and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged in the schools e-safety incident report book and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing body

The IT manager/s

The IT manager/s are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics - Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet - Childnet International: https://www.childnet.com

Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

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

- 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

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and social media pages. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher

Cyber-bullying

Definition

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.)

Preventing and addressing cyber-bullying

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. Class Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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

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 endeavors to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet and IT systems in school

Expectations of the IT User

The following guidelines set Homefield Primary School ’s expectations for the acceptable use of equipment and use of computers generally around the school by staff and pupils. Access to the networked resources is a privilege, not a right. Users are responsible for their behavior and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to The Network Manager/s.

We have created “Acceptable Use Agreement for Pupils” which, has been designed with the children in mind, for them to understand quickly and easily what is and is not acceptable. Parents/Carers are asked to sign the Acceptable Use Agreement before their child uses the Internet in school.

Staff are expected to sign the Acceptable Use Agreement upon induction.

Passwords

The school has a password policy that staff must adhere to. This is to protect the network from unauthorised attack and to secure our data. Your password must be made up of the following:

- 7 characters or more
- Contains at least 1 number, 1 capital letter and 1 special character

- Does not contain your name or username
- Is unique to the school's network and not used anywhere else

Unacceptable Files – On a regular basis the IT Systems Manager/s will search the network for illegal or unacceptable files; which in turn will be removed.

Network Etiquette and Privacy

Users are expected to utilise the network systems in a responsible manner. All computer systems are restricted and regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school code of conduct

Social Media

I will

- Be aware damage to professional reputations can inadvertently be caused by quite innocent postings or images
- be aware and careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children.
- I will support and promote the school's e-safety and data protection policies and help students be safe and responsible in their use of the Internet and related technologies.
- I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. If this happens, I will report it immediately to the IT Manager and through the schools CPLO channels.
- Ensure that any comments or posts about the school or County Council must state that it is an expression of your own personal view.

IT Equipment

I will

- not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
- ensure that portable ICT equipment such as laptops, digital still and video cameras are put back in their correct storage locations when not being used.
- not attempt to harm or destroy any equipment or data of another user or network

connected to the school system.

- understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
- not use “USB drives”, portable hard-drives or personal laptops on the network without first discussing it with the IT Manager.
- if equipment is faulty or damaged it report it immediately to the IT manager, I will not attempt to fix it myself.
- not allow pupils to use any printers or equipment that requires specific training to use.

Network & Web Browsing

I will

- not attempt to gain access to files & folders that I do not explicitly have access to.
- not use the network in any way that would disrupt use of the network by others.
- Report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the IT Manager
- not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
- not continue using the machine if I find an unattended machine logged on under other users username – I will log it off immediately.
- ensure that I log off after my network session has finished.
- not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

Email & Data Privacy

- I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
- I will not send or publish material that violates General Data Protection Regulations (GDPR) or breaching the security this act requires for personal data.
- I will ensure that any Personal Data (where the GDPR applies) that is sent over the Internet will be encrypted or otherwise secured. If you intend to do this please ensure the

process has first been approved by the IT manager.

- I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
- I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person. I will not reveal any of my personal information to students.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
- I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the IT Manager.
- I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

- I am aware that I must comply with the acceptable use policy of any other networks that they access.
- It is your responsibility to report anything that you suspect may be in breach of these rules to the IT manager

Hacking

Hacking into or attempting to corrupt the network settings, software or hardware will not be tolerated. Any attempts to do so will be picked up through regular network checks and will be dealt with by a member of the Senior Leadership Team.

Use of the Internet and e-mail

Homefield Primary School uses a filtered, broadband internet service provider for e-mail and internet access. Pupils and staff will be allowed to use the internet to search for information and resources to meet their professional and learning objectives in school. Pupils and staff will need to be aware that there is no regulatory authority body for the internet, anyone, anywhere can publish materials. It is not censored for opinion, bias or validity of information.

All members of staff must read the West Sussex Guidance for The Safer Use of the Internet by Staff working with Young People a copy of which is held in the school office.

Reporting Faults

All faults with IT Systems at Homefield Primary School must be reported to the IT Manager/s, even if it's a fault that can be fixed by yourself, for example, restarting a computer please still report this as it could reoccur or lead to further issues.

If equipment that results from fault or breakage (broken iPad screen, strange noises, smoke) poses an immediate health and safety risk it is your responsibility to minimise the risk exposed and report it. For example:

- Broken iPad screen; put the iPad in a place out of reach of children, then bring it to the IT Manager.
- Strange noise from projector; turn off the projector, at the power source if possible and report it to the IT Manager
- Smoke imitating from a computer, sound the fire alarm immediately and if safe to do so isolate the power. Report this to the fire marshal.

Raising Faults

Faults are required to be raised in the following processes to come under the Service Level Agreement:

- Emailing itsupport@homefield-primary.co.uk
- Any faults raised outside of these processes (i.e word of mouth, speaking to us in person when outside of the office or notes left on desks) do not fall under the SLA.

Extraordinary Circumstances

If equipment is damaged by external sources (fire, water, electricity or stolen through theft) then the SLA timings will not apply but a review will be done to ensure the parties effected will know an estimated fix time when services will be operational.

Guidance for school staff regarding social networking sites outside of school

For those who belong to a social networking site (eg Facebook, Twitter, My Space) there are some important issues to note if you want to protect yourself.

- Do not accept any contact with current or previous pupils
- If under 18s are on your list (perhaps family members) be especially careful that the content is appropriate, including photos
- Avoid bad language, sexual connotations, obscene jokes
- Avoid criticism of your employer

- Do not post photos of colleagues without their prior permission
- Check privacy settings and do not post comments that may bring your professional status and the school into disrepute.
- Do not be friends with parents/carers or children you have met through your work at Homefield Primary School

Remember these sites are not always private - often there is a wide access. Ensure that your privacy settings are set to private. Do not say anything that you would not say in public or post comments associated with school which could be easily construed as a breach of confidentiality or even bullying. This is especially important as there have been cases across the country where people have been found to be showing "poor judgment" in relation to professional conduct and/or safeguarding which may be recorded on their permanent record which could affect references.

Use of Digital Images

For the purposes of this section publication includes on websites, including social media, in the press, on TV, as web broadcasts or video to be released into the public domain.

- Written permission from parents or carers must be submitted to the school before any photo, recording or child's work can be used on the internet including social media sites and local news publicity.
- Named images of pupils must not be published in any circumstance. This includes photographs, videos, TV presentations, web pages, social media, the press etc.
- The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' work can be published (e.g. photographs, videos, TV presentations, web pages, press etc.) unless parental objection has been provided in writing.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Mobile Phone and Device Use

The role of staff

All staff should consistently enforce the school's policy on the use of mobile phones and smart watches. Staff should not use their own mobile phone or smart watch in front of pupils throughout the school day. Staff can check their phones/watch in empty classrooms, the staff room, or offices. This will empower staff to better challenge pupils to meet the school expectations and effectively enforce the prohibition of mobile phones throughout the school day.

The role of pupils

All pupils should be clear that it is the school's policy that the use of mobile phones/smart watches whilst at school is prohibited. When children enter the classroom upon arrival at school, they will be expected to hand over their named phone to their class teacher who will store this securely in a locked box. The consequences of not following this rule or for using a smart watch for anything other than telling the time will be a meeting with the child's parents and the device potentially being banned for that child.

Pupils should be taught the risks that are associated with the use of mobile phones and smart watches, both in school and more broadly, to ensure they understand the decision being taken by the school to prohibit the use of them throughout the school day. These risks can include a loss of focus in lessons, classroom disruption and an increase in bullying.

Pupils should also be taught the benefits of having a mobile phone-free environment and be encouraged to see such an environment as desirable and valuable. This will help to create intrinsic motivation to support the school culture.

The role of parents

Parents have an important role in supporting the school's policy on prohibiting the use of mobile phones and should be encouraged to reinforce and discuss the policy at home as appropriate, including the risks associated with mobile phone use and the benefits of a mobile phone-free environment.

Where parents need to contact their child during the school day, they should be directed to the school office, where staff will be aware of the school's policy on relaying messages and facilitating contact. Where parents have questions or concerns, staff should address these in a timely manner and clearly communicate the reasons for prohibiting the use of mobile phones.

Volunteers, Visitors, Governors and Contractors

All Volunteers, Visitors, Governors and Contractors are expected to follow our mobile phone and device policy as it relates to staff whilst on the premises. Notices are placed around the school advising this.

Staff using work devices outside school

All staff with access to a school device for use outside of school will be asked to sign a consent form.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT manager/s.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

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

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online in the schools e-safety incident report book

This policy will be reviewed annually by the DSL/IT Manager. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Remote Learning policy