Simul autem et crescere luceat
Together we grow and shine

Fountain Head House School
Online Safety Policy

Review due	June 2024
Last review	June 2023
Reviewed by	Thereza de Lucca Headteacher
Approved by	Julie Smith Chair of the Board

Contents	Page
Aims	3
Definitions	3
Legislation and guidance	3
Roles and responsibilities	4
Educating pupils about online safety	5
Informing parents and carers about online safety	5
Cyber-bullying	6
Acceptable use of the internet in school	7
Pupils' use of mobile devices in school	7
Visitors' use of mobile devices in school	8
Staff's use of mobile devices in school	8
Staff's use of work devices outside school	8
How the school will respond to issues of misuse	8
Training	9
Links to other policies	9
Appendix 1 ICT and mobile phone acceptable use - guidance for pupils	10
Appendix 2 Facebook concise guidance for staff	11

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, including mobile and smart technology (which we refer to as 'mobile devices')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Definitions

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 pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **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 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

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

Roles and responsibilities

The Headteacher

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

The Headteacher is responsible for ensuring that teaching about safeguarding, including online safety, is relevant, sequential and adapted to the pupils' special educational needs and/or disabilities (SEND), specific vulnerabilities and level of ability and understanding of each pupil in the school. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Designated Safeguarding Lead (DSL)

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Business Manager and other staff, as necessary, to address any online safety issues or incidents
- Working with the PSHE Lead regarding the Online Safety aspects of the PSHE Curriculum and delivering Online Safety lessons to pupils across he school
- 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 logged and dealt with appropriately
- Updating and delivering staff training on Online Safety
- Liaising with other agencies and/or external services if necessary
- Reporting on Online Safety incidents as appropriate

The Business Manager

The Business Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring that the IT service provider conducts full security checks and monitoring of the school's ICT systems regularly.
- Ensuring that the school has appropriate filters in place to block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are recorded and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately

All staff

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Following the school's ICT and Internet Acceptable Use Policy, including guidance for staff and pupils
- Working with the DSL to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Following the guidance in the school's ICT and Internet Acceptable Use Policy, including guidance for parents and carers, and pupils
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Educating pupils about online safety

At FHHS, educating pupils about online safety is an essential aspect of our PSHE Curriculum. Our PSHE Curriculum Framework is based on the *PSHE Education Framework for Pupils with SEND – PSHE Association*, and includes all statutory Relationships Education (Primary), Relationships and Sex Education (Secondary) and Health Education (Primary and Secondary) content adheres to three core strands in line with the Department for Education: Health & Wellbeing; Living in the Wider World; Relationships.

Using resources from the PSHE Association, Learn Brook and Jigsaw (provision for nursery and EYFS) the planning of the PSHE curriculum takes a thematic approach to primary PSHE education. The curriculum that we offer at FHHS is split into three core elements, these are:

1. **Health and Wellbeing**: puberty, mental health, keeping active, dental care and healthy eating.
2. **Relationships**: respectful and healthy relationships (both on and offline), kindness and sex education.
3. **Living in the Wider World**: career planning, financial literacy and exploring our rights and responsibilities.

The curriculum that we follow offers a programme including statutory Relationships and Health Education, in a spiral, progressive and fully planned scheme of work, whilst giving the children relevant learning experiences to help them navigate their world and to develop positive relationships with themselves and others.

With a strong emphasis on emotional literacy, building resilience and nurturing mental and physical health, the PSHE curriculum equips FHHS to deliver engaging and relevant PSHE within a whole-school approach.

The curriculum provision allows different year groups to work on the same themes at the same time, building a spiral program year on year, whilst offering flexibility to respond to intelligent informed PSHE events.

Informing parents and carers about online safety

The school will raise parents and carers' awareness of online safety through updates on the school's Facebook page; communications via email or other relevant opportunities. This policy will also be shared with parents.

If parents and 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.

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.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we include learning in our PSHE Curriculum to help pupils understand what it is and what to do if they become aware of it happening to them or others. We encourage pupils to report any incidents to a trusted adult, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, not only as part of PSHE learning but also in any other relevant learning opportunities.

Cyber-bullying is included in Safeguarding Training for staff. The school also shares relevant information about cyber-bullying with parents and carers as part of a whole approach to online safety.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy and Safeguarding and Child Protection 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 DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the Headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has 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

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or any other relevant member of the Senior Leadership Team
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation an if the pupil refuses to co-operate follow the school's Behaviour Policy

The authorised staff member should:

- Inform the DSL (or DDSL) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or DDSL) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has, or could be used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher, the DSL or any member of the Safeguarding Team 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 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
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening 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
- The school's Behaviour Policy
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school's Complaints Policy and Procedures.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to follow the school's ICT and Internet Acceptable Use Policy. Visitors will be expected to follow the acceptable use guidance if relevant.

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 will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils' use of mobile devices in school

Pupils are allowed to bring mobile phones in to school but they **must** hand them in at arrival for safe keeping during the school day. Pupils' mobile phones will be safely kept either in a locked storage area in our near the classroom or at the school's office area depending on appropriateness.

It is understood that some pupils might present anxiety regarding the ability to contact parents. Where this is the case, there will be an agreement which allows pupils to request to contact their parents for emergencies.

As part of this agreement, it will be stated that the use of mobile phones will take place out of the learning areas in a quiet space with staff supervision.

Important messages and phone calls to or from parents can be made at the school phone or SLT work mobiles. The school ensures that messages from parents to pupils and pupils to parents are communicated and followed up.

Visitors' use of mobile devices in school

Visitors to the school include parents and carers, contractors, external professionals, and any other persons entering the school site.

Visitors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

During school events, parents and carers are asked not to take photographs or videos. The school will take photos of school events and share these with parents and carers as appropriate.

Staff's use of mobile devices in school

All staff should leave their personal mobile phones in a locker or other secure place and not on their person and only use them in private staff areas during school hours.

Child/staff data should never be downloaded onto a personal phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may request via their line manager that they keep their mobile phone close to hand. This will always be on silent or vibrating alert mode.

Staff's use of work devices outside school

Work devices include mobiles, laptops, tablets. All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.

How will the school respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy and ICT and Internet Acceptable Use 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 ICT 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 Code of Conduct. 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 and Weekly Staff Briefings).

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

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL 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.

Links to other policies

This policy should be read alongside the school's policies on:

- FHHS – PSHE (including RSHE) Policy
- FHHS – ICT and Internet Acceptable Use Policy
- FHHS – Mobile Phone and Personal Device Usage Policy
- FHHS – Safeguarding and Child Protection Policy
- FHHS – Behaviour Policy
- FHHS – Staff Code of Conduct
- FHHS – Data protection Protection Policy

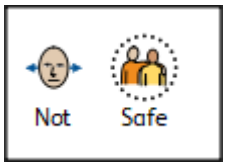
Appendix 1 - ICT and mobile phone acceptable use – guidance for pupils

ICT and mobile phone acceptable use – guidance for pupils

All pupils must use school ICT systems in a safe and responsible way

To keep myself safe, I will

- Hand my mobile phone in at the start of the day
- Speak to an adult about anything that worries me online or does not feel right
- Be kind towards others online
- Treat others online in the same way that I would like to be treated online
- Treat equipment carefully and in the same way that I would treat my own equipment at home. I will report any damages
- Keep my email password to myself



To keep myself safe, I will not

- Speak to strangers online
- Arrange to meet people in person that I have met online
- Use the internet or social media to be unkind to or about others
- Use aggressive or inappropriate language when communicating online
- Be unkind about other pupils' work online
- Use social media to pretend to be someone else
- Upload or download any inappropriate material
- Open email attachments from people that I do not know
- Log on any other person internet email account

Appendix 2 - Facebook Concise Guidance for Staff

Do not accept friend requests from pupils on social media

Advice for school staff on Facebook

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
- Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional
- Check your privacy settings regularly
- Be careful about tagging other staff members in images or posts
- Don't share anything publicly that you wouldn't be just as happy showing your pupils
- Don't use social media sites during school hours
- Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
- Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
- Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
- Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police