# Hartsfield JMI School

# Online Safety Policy

**Based on HfL model Policy June 2020-**

**confirmed as reviewed and no changes noted as of September 2024.**

**Updates based on changes in DDSL for January 2025**

| | |
|---|---|
| Approval Date:<br><br>December 2024 | Review Date:<br><br>December 2026 |
| <br><br>Name:<br>Role: | Written by: School<br><br>Philippa Smith<br>Headteacher |
| <br><br>Name:<br>Role: | Approved by: Governing Body<br><br>Sian Chrimes<br>Chair of Governors |

# Contents


1. Introduction
2. Responsibilities
3. Scope of Policy
4. Policy & Procedures
5. Curriculum
6. Staff and Governor Training
7. Working in Partnership with Parents & Carers
8. Records, Monitoring and Review
9. Appendices of the Online Safety Policy:
    A. Online Safety Acceptable Use Agreement – Staff, Governors and Student Teachers
    B. Online Safety Acceptable Use Agreement – Peripatetic Teachers, Coaches and Supply Teachers
    C. Requirements for Visitors, Volunteers and Parent/Carer Helpers
    D. Online Safety Acceptable Use Agreement for Primary Pupils
    E. Online Safety Policy Guide – Summary of Key Parent/Carer Responsibilities
    F. Guidance on the Process for Responding to Cyberbullying Incidents
    G. Guidance for Staff on Preventing and Responding to Negative Comments on Social Media
    H. Online Safety Incident Form
    I. Online Safety Incident Log

## 1. Introduction

Hartsfield School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play, but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

## 2. Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is Philippa Smith, Headteacher.
All breaches of this policy must be reported to Philippa Smith, Headteacher.
All breaches of this policy that may have put a child at risk must also be reported to the DSL, Philippa Smith.
Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

## 3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff

- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in education, Data protection, health and safety, home–school agreement, home learning, and behaviour/ anti-bullying policies.

## 4. Policy and Procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

### Use of Email

Staff and governors should use a school email account or Governorhub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Protection policy. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Philippa Smith, Headteacher.

**Users must not** send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

**Visiting Online Sites and Downloading**

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content.

- When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

**Users Must Not**:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

**Users Must Not:**

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school

- Use the school's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others

- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

A monitorable system would be one such as our remote desktop server. Through our remote desktop server any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user logs-out of our remote desktop server, there are no copies left on their own device.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Philippa Smith, Headteacher.

**Storage of Images**

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See data Protection policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by Philippa Smith, Headteacher.

Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. The only exception is the taking of images on personal mobile devices using the application DS File which stores the images once taken on the school server. This will require permission of the Headteacher before use. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file. Any photos or data recorded on personal devices for short term operational use within school, must be deleted from those devices before the end of the same school day.

**Use of Personal Mobile Devices (including phones)**

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas, as identified by the Headteacher, and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers and visitors may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Philippa Smith, Headteacher. When a parent/carer or visitor is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. All such devices must be named and switched off and stored by the school during the school day. At Hartsfield, under no circumstance should pupils use their personal mobile devices/phones to take images of any other pupil any member of staff.

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access school emails and data. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

### New Technological Devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with Philippa Smith, Headteacher before they are brought into school. Any photos or data recorded on personal devices for short term operational use within school, must be deleted from those devices before the end of the same school day.

### Reporting Incidents, Abuse and Inappropriate Material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL Philippa Smith, or Deputy DSLs, Clare Nelson or Lauren Nosal (from January 2025). Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

## 5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities

e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images

- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

## 6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix E).

## 7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement on entry to the school. Parents/carers are further signposted when changes are subsequently made. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

## 8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Online safety incident recording formats are provided in appendices I, J and K for schools that wish to use them.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents if they occur for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on scheduled policy review and on an annual basis as part of the annual GDPR reporting.

## 9. Appendices to the Online Safety Policy

A. Online Safety Acceptable Use Agreement - Staff, Governors and Student Teachers (on placement or on staff)

B. Online Safety Acceptable Use Agreement - Peripatetic Teachers/Coaches, Supply Teachers

C. Requirements for Visitors, Volunteers and Parent/Carer Helpers Working in the School (Working Directly with Children or Otherwise)

D. Online Safety Acceptable Use Agreement Primary Pupils

E. Online Safety Policy Guide - Summary of Key Parent/Carer Responsibilities

F. Guidance on the Process for Responding to Cyberbullying Incidents

G. Guidance for Staff on Preventing and Responding to Negative Comments on Social Media

H. Online Safety Incident Reporting Form

I. Online Safety Incident Log

## Appendix A -Online Safety Acceptable Use Agreement - Staff, Governors and Student Teachers (on Placement or on Staff)

You must read this agreement in conjunction with the online safety policy and the Data Protection Policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Philippa Smith, Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

**Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to Philippa Smith, Headteacher (DSL) or Deputy DSL and an incident report completed.

**Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Philippa Smith, Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

**Social Networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

**Passwords**

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

**Data Protection**

I will follow requirements for data protection as outlined in the Data Protection Policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

**Images and Videos**

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

The use of cloud based or other video conferencing services is permissible for staff, professional or governor meetings/interviews with the prior consent of the Headteacher. Decisions about whether to retain images will be made by the Headteacher dependant on the circumstances.

I will not take images, sound recordings or videos of school events or activities on any personal device unless specific permission has been granted.

**Use of Email**

I will use my school email address or Governorhub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email address/es or Governorhub for personal matters or non-school business.

**Use of Personal Devices**

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher. The taking of images on personal mobile devices using the application DS File which stores the images once taken on the school server is permitted. This will require permission of the Headteacher before use. Any photos or data recorded on personal devices for short term operational use within school, must be deleted from those devices before the end of the same school day.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security

A ‘monitorable system’ would be one such as our remote desktop server. Through our remote desktop server, any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user logs-out of our remote desktop server, there are no copies left on their own device.

**Additional Hardware/Software**

I will not install any hardware or software on school equipment without permission of Philippa Smith, Headteacher.

**Promoting Online Safety**

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL Philippa Smith or Deputy DDSLs, Clare Nelson or Lauren Nosal.

**Classroom Management of Internet Access**

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Philippa Smith, Headteacher.

**Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership ,DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

**User Signature**

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature ……..……..…… Date ……

Full Name ……..... (Please Print)

Job title ……..……

## Appendix B - Online Safety Acceptable Use Agreement - Peripatetic Teachers/Coaches, Supply Teachers

**School Name:** Hartsfield JMI School

**Online Safety Lead:** Philippa Smith- Headteacher

**Designated Safeguarding Lead (DSL):** Philippa Smith

**Deputy Designated Safeguarding Leads (DDSL):** Clare Nelson and Lauren Nosal

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Philippa Smith, Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

**Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

**Online Conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Philippa Smith, Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with Philippa Smith, Headteacher.

**Social Networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.
I will not upload any material about or references to the school or its community on my personal social networks.

**Passwords**

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

**Data Protection**

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

**Images and Videos**

I understand that I may make sound recordings of pupils work for sharing with that pupils' parents' providing they cannot be identified from the recording. I will not make or upload video or image recordings of pupils without the Headteachers' specific consent.

The use of cloud based or other video conferencing services is permissible for remote teaching, staff, professional or governor meetings/interviews with the prior consent of the Headteacher. No images will be recorded or stored from these sessions unless they are for the purpose of teaching pupils remotely. When teaching pupils remotely, some things to consider when delivering virtual lessons, especially where webcams are involved include:

- Parents must be present and visible during all virtual teaching sessions.
- Pupils must be taught in groups wherever possible.
- Staff and pupils should must wear appropriate clothing, as should anyone else in the household.

- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by Hartsfield to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held.

**Use of Email**

I will use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

**Use of Personal Devices**

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas for school purposes to support my role in childrens' learning.

**Additional Hardware/Software**

I will not install any hardware or software on school equipment without permission of Philippa Smith, Headteacher.
.

**Promoting Online Safety**

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL Philippa Smith or the Deputy DSLs, Clare Nelson or Lauren Nosal.

**Classroom Management of Internet Access**

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Philippa Smith, Headteacher.

**Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership ,DPO and DSL. A school-owned device should be used when running video-conferences, where possible

**User Signature**

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..……..…… Date ……

Full Name ……..... (Please Print)

Job title ……..……

**Appendix C - Requirements for Visitors, Volunteers and Parent/Carer Helpers**

**(Working Directly with Children or Otherwise)**

**School Name:** Hartsfield JMI School

**Online Safety Lead:** Philippa Smith Headteacher

**Designated Safeguarding Lead (DSL):** Philippa Smith

**Deputy Designated Safeguarding Leads (DDSL):** Clare Nelson or Lauren Nosal

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher and/or DDSP.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSP/Headteacher or DDSP is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

## Appendix D - Online Safety Acceptable Use Agreement Primary Pupil

## My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher.
- I will only open email attachments when it has been approved by a member of school staff in school or a parent/carer out of school.
- I will only open or delete my school files when told by a member of staff or a parent.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact that I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parents'/carers' permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.

- I understand my behaviour in the virtual classroom should mirror that in the physical classroom
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

**Dear Parent/Carer,**

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign it to say that you agree to follow the rules. Any concerns or explanation can be discussed with The Headteacher, Mrs. Philippa Smith.

Please return the signed sections of this form which will be kept on record at the school.

**Pupil Agreement**

**Pupil Name……**

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

**Pupil Signature……**

**Parent/s Carer/s Agreement**

**Parent/s Carer/s Name/s……**

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.)

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

**Parent/Carer Signature……..**

**Date ……**

**Appendix E - Online Safety Policy Guide - Summary of Key Parent/Carer Responsibilities**

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- A parent must be present and visible during all virtual teaching sessions.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

## Appendix F - Guidance on the Process for Responding to Cyberbullying Incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

## Appendix G - Guidance for Staff on Preventing and Responding to Negative Comments on Social Media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide) - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

Collect the facts:
As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

Addressing negative comments and complaints:

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available. The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

Reporting the matter to the social network site if it breaches their rules or breaks the law;

Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law.  Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

# Appendix H - Online Safety Incident Form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to Philippa smith (Headteacher).

| | | | | |
|---|---|---|---|---|
| Name of person reporting incident: | | | | |
| Date of report: | | | | |
| Where did the incident take place: | Inside school? | | Outside school? | |
| Date of incident(s): | | | | |
| Time of incident(s): | | | | |

| Who was involved in the incident(s)? | Full names and/or contact details |
|---|---|
| Children/young person | |
| Staff member(s) | |
| Parent(s)/carer(s) | |
| Other, please specify | |

| Type of incident(s) (indicate as many as apply) | | | |
|---|---|---|---|
| Accessing age inappropriate websites, apps and social media | | Accessing someone else's account without permission | |
| Forwarding/spreading chain messages or threatening material | | Posting images without permission of all involved | |
| Online bullying or harassment (cyberbullying) | | Posting material that will bring an individual or the school into disrepute | |
| Racist, sexist, homophobic, religious or other hate material | | Online gambling | |
| Sexting/Child abuse images | | Deliberately bypassing security | |
| Grooming | | Hacking or spreading viruses | |
| Accessing, sharing or creating pornographic images and media | | Accessing and/or sharing terrorist material | |
| Accessing, sharing or creating violent images and media | | Drug/bomb making material | |
| Creating an account in someone else's name to bring them into disrepute | | Breaching copyright regulations | |
| Other breach of Acceptable Use Agreement | | | |
| Other, please specify | | | |

| | |
|---|---|
| Full description of the incident | What, when, where, how? |
| Name all social media involved | Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc |
| Evidence of the incident | Specify any evidence provided but do not attach |

**Thank you for completing and submitting this form.**

## For completion by DSL/Headteacher/ DDSL

| Immediate action taken following the reported incident: | |
|---|---|
| Incident reported to DSL/Headteacher/ DDSL | |
| Safeguarding advice sought, please specify | |
| Referral made to HCC Safeguarding | |
| Incident reported to police and/or CEOP | |
| Online safety policy to be reviewed/amended | |
| Parent(s)/carer(s) informed please specify | |
| Incident reported to social networking site | |
| Other actions e.g. warnings, sanctions, debrief and support | |
| Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery | |

| | |
|---|---|
| **Brief summary of incident, investigation and outcome (for monitoring purposes)** | |

## Appendix I - Online Safety Incident Log

Summary details of ALL online safety incidents will be recorded on this form by the online safety Lead or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

| Date & time | Name of pupil or staff member<br>Indicate target (T) or offender (O) | Nature of incident(s) | Details of incident<br>(including evidence) | Outcome including action taken |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |