




HPP

Online Safety Policy

This policy was reviewed:	January 2023
This policy will be reviewed again:	Spring 2024
Governor Committee Responsibility:	School Improvement
Statutory policy?	No
Source:	School

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL) team	Claire Cook (HISN), Jon James (HJS)
	Delegated Online-safety leads	Safia Ashak (HISN), Daisy Peaty (HJS)
	Online-safety / safeguarding link governor	Emily Boswell and Polly Davies
	PSHE/RSHE lead	Amber Tullet (HISN), Thea Woolf (HJS)
	Network manager / other technical support	Click on IT
	Date this policy was reviewed and by whom	January 2023 by Jon James, Claire Cook, Daisy Peaty and Safia Ashak
	Date of next review and by whom	Spring 2024 by Daisy Peaty and Safia Ashak

Overview

Aims

This policy aims to:

- Set out expectations for all HPP community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope

This policy applies to all members of the HPP community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Executive Headteacher – Helen Lockey

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements (see appendices for website audit document)

Designated Safeguarding Lead / Online Safety Lead/Head of School – Claire Cook (HISN) and Jon James (HJS)

- Work with the Executive Headteacher and technical staff to review protections for **remote-learning** procedures, rules and safeguards (pupils using school accounts at home have school strict restricted youtube access applied).
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Stay up to date with the latest trends in online safeguarding

- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework '[Education for a Connected World – 2020 edition](#)') and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents
- Communicate regularly with SLT and the designated safeguarding governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown. Ensure the updated 2022 [DfE guidance on Keeping children safe in education](#) is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Ensure all staff complete an annual online safeguarding training.

Governing Body, led by Safeguarding Link Governor – Emily Boswell and Polly Davies

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2021)

- Approve this policy and strategy and subsequently review its effectiveness,
- Ask about how the school has reviewed protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards.

All staff

Key responsibilities:

- In 2021 pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technology**.
- Understand that online safety is a core part of safeguarding
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures on CPOMS.
- Sign and follow the staff acceptable use policy and code of conduct/handbook.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- When supporting pupils remotely, be mindful of additional safeguarding considerations.

- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology.
- To complete an annual online safeguarding training.

PSHE / RSHE Lead/s – Amber Tulett (HISN) and Thea Woolf (HJS)

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should now be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – Safia Ashak (HISN) and Daisy Peaty (HJS)

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
- Work closely with the PSHE subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Network Manager/technician – CITL London

Key responsibilities:

- Maintain up-to-date documentation of the school's online security and technical procedures
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Reactively monitor the use of school technology, online platforms and that any misuse/attempted misuse having been identified and reported in line with school policy.

Data Protection Officer (DPO) –Lauren Drake

Key responsibilities:

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session**, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy

- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

External groups including parent associations – HISNA and FOHJS

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school

- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

At HPP, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding.

General concerns must be handled in the same way as any other safeguarding concern and reported to the DSL, followed by logging the incident on CPOMS.;

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy
- Positive Behaviour Policy

- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

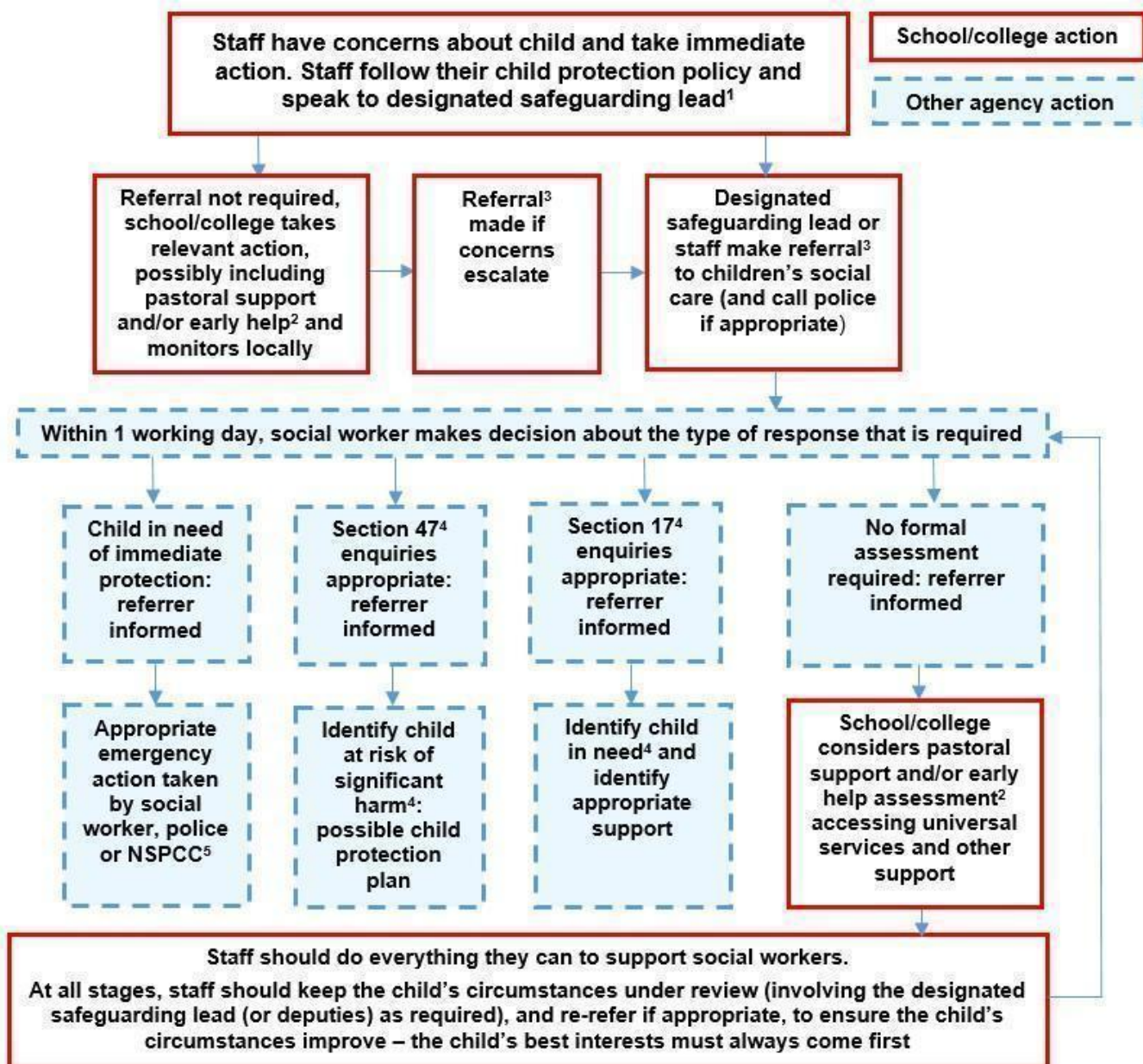
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (you may want to display a poster with details of this / other helplines in the staff room).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

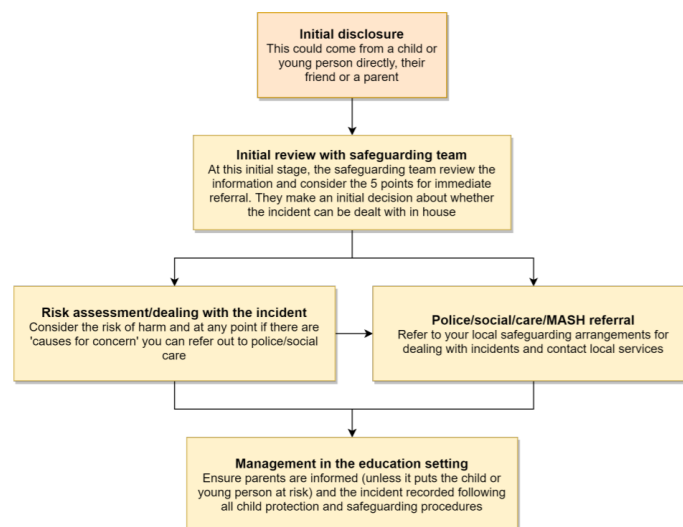


Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#) to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved.



*Consider the 5 points for immediate referral at initial review:

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the Positive Behaviour Policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy (see appendix A) as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as a 'bring your own device agreement' (see appendix A).

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the HPP community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, HPP the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Egress and Meraki Mobile Device Management (ipads).

The headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies where there is a legal basis for doing so. . Whilst basic information (name, DOB) can be shared internally within the Partnership and with AfC by email, staff should use USO-FX / Egress to encrypt a the most sensitive of pupil data, including medical and safeguarding information. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

The internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.

Additional safeguards in place are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access

Electronic communications

Email

- Staff at this school use the Education GMail system for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email and Google Meet are the only means of electronic communication to be used between staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / head of school in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Executive Headteacher (if by a staff member).
- Email may only be sent using the email system above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately. Google Meet can only be used through Education account.
- Staff or pupil personal data should never be sent/shared/stored on email.
 - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
 - Internally, staff should use the school network, including when working from home when remote access is available via Google Workspace (previously G Suite).
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Executive Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Caroline Maloney (HISN) and office team (HJS). The site is managed by / hosted by School Website Design Agency. (NB Google classrooms are updated by class teachers).

The DfE has determined information which must be available on a school website. Where other staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – Where pupil work, images or videos are published on the website, their identities are protected and full names are not published

Cloud platforms

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos,

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites

Whenever a photo or video is taken/made, the member of staff taking it will check the latest Integris database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At HPP, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services

Photos are stored on the school network/Google drive in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

HPP's SM presence

HPP works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner even though there are no official/active school social media accounts. HISNA and FOHJS are responsible for their online presence in line with the school's AUP.

Staff, pupils' and parents' SM presence

Social media is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve). Class reps monitor the Whatsapp groups and are responsible for closing down inappropriate content.

Staff and Governors should not accept 'friend' request on any social media platforms from any present pupils, or past pupils who are still under the age of 18. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Executive Headteacher, and should be declared upon entry of the pupil or staff member to the school.

Device usage

Personal devices including wearable technology

- **Pupils/students** who walk alone to school in HJS are allowed to bring mobile phones in for emergency use only, but not when moving around the school buildings. During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Pupils are not allowed to wear/bring SMART watches to school.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas (empty room or office or staff room) during school hours. After school they can be used anywhere as long as there are no pupils present at clubs.
- **Volunteers, contractors, governors** 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 Executive Headteacher should be sought (the executive headteacher may choose to delegate this to Heads of School) and this should be done in the presence of a member staff.
- **Parents** can use mobile phones on site when collecting pupils but they cannot take pictures. At school events parents are given appropriate reminders about mobile phone usage. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours.
- **Governors** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy.
- **Volunteers, Contractors, Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, all communication with parents will be conducted through the school office. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Other Linked Policies

1. Safeguarding and Child Protection Policy
2. Behaviour Policy / Anti-Bullying Policy
3. Staff Code of Conduct / Handbook
4. Acceptable Use of ICT
5. Data protection Policy
6. Behaviour Policy
7. Bullying Policy

Appendix A: Acceptable use of technology agreement.

HPP staff acceptable use agreement

Staff Acceptable Use of Information and Communications Technology Agreement

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct agreement.

- I have read and understood the Hampton Junior School Online Safety Policy.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content, they access or create.
- I will complete a yearly online safety training with the National College.

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

Pupil and parent agreement – Hampton Infant School & Nursery



Hampton Infant School & Nursery



Pupil and Parent Agreement Acceptable use of Information and Communications Technology

We understand that your child is too young to give informed consent on his/her own but feel it would be good practice to involve the children as much as possible when it comes to keeping them safe online.

Please could you spend 10 minutes reading through the E-Safety Agreement with them and discussing the importance of each statement.

Any concerns that you may have regarding E-Safety can be reported to our Designated Safeguarding Lead, Mrs Claire Cook.

E-Safety Agreement Statements for Children

I only use the devices I'm ALLOWED to.
I CHECK before I use new sites, games or apps.
I ASK for help if I'm stuck.
I THINK before I click.
I KNOW people online aren't always who they say.
I don't keep SECRETS just because someone asks me to.
I am RESPONSIBLE so I never share private information.
I am KIND and polite to everyone.
I TELL a trusted adult if I'm worried, scared or just not sure.

Parent's Agreement

I have read and understood the E-Safety agreement and will encourage my child to abide by these rules.

I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate material.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have any concerns over my child's E-Safety.

I will ensure that any pictures taken at school events will not be shared on any social media platforms.

By completing the **HISN New Pupil Information [eform](#)**, you confirm that both you and your child have read, understand and agree to comply with this agreement.

Pupil and Parent Agreement
Acceptable use of Information and Communications
Technology Agreement

Pupil

When I use the Internet, social media and email, I will keep to these rules:

- I will only use the Internet with permission and only when there is a teacher or member of HJS staff present
- I will not try to find unsuitable sites on the Internet and I will keep away from sites that I am not permitted to access.
- I will only email people I know or who my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my full name or home address or telephone number, or arrange to meet someone unless my parent, carer, or teacher has given written permission.
- I will keep passwords safe.
- I will keep my parents and responsible adults in school informed of anything that upsets me when using technology.

Parent

I have read and understood the above rules for acceptable use of the Internet and will discuss these with my child.

By completing the New Pupil Information Form, you confirm that both you and your child have read, understand and agree to comply with this agreement.

Appendix B: Permission to bring a mobile phone into school agreement.

Permission to bring a mobile phone into school

Whilst we understand the need for some children in year 5 and 6 to bring in their mobile phone/smart watch to school, we must remind parents/carers of the following:

We can only accept mobile phones/smart watches where an adult has completed this form.

- ☐ Mobile phones/smart watches should be handed to the class teacher before the start of school for safe keeping and collected at the end of the day
- ☐ The mobile phone/smart watch should be clearly marked with the child's name and switched off.
- ☐ Mobile phones/smart watches should not be used on HJS premises before or after school.
- ☐ The school accepts no responsibility for damage or loss of mobile phones/smart watches.

Any child not adhering to the above procedures will have their mobile phone/smart watch confiscated

If there are extenuating circumstances for a year 3 or 4 child to bring a mobile phone/smart watch to school, prior permission must be sought from the Executive Leadership Team.