Prior Heath Infant School

Online Safety Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Key Staff

Headteacher/Designated Safeguarding Lead:	Lindsey Chivers
Deputy Designated Safeguarding Lead:	Sarah Haygarth
Computing lead (with responsibility for Online safety):	Rachel Bates
Technology Governor:	Mark Prentice

Date created: June 2025
Next review date: June 2026

This Online Safety Policy outlines the commitment Prior Heath Infant School has to safeguard members of our school community online in accordance with statutory guidance and best practice.

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- Describes how the school will help prepare pupils to be safe and responsible users of online technologies.
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- Is supplemented by a series of related acceptable use agreements.
- Is made available to staff at induction and through normal communication channels.
- is published on the school website.

This Online Safety Policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Prior Heath Infant School will deal with such incidents within this policy and associated Positive Behaviour and Anti-Bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	10th June 2025
The implementation of this Online Safety Policy will be monitored by:	Headteacher: Lindsey Chivers Computing Lead (with responsibility for Online Safety) : Rachel Bates Technology governor: Mark Prentice
Monitoring will take place:	Once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	June 2026
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Headteacher and DSL: Mrs. Chivers Deputy DSL: Mrs. Haygarth LADO: 03001231650- Single Point of Access on 0300 470 9100. email:education.safeguarding@surreycc.gov.uk Telephone: 01483 517771

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Filtering and monitoring logs.
- Internal monitoring data for network activity.
- Surveys/questionnaires of:
    - pupils
    - parents and carers
    - staff.

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding. The Headteacher, as DSL, also has the day-to-day responsibility for online safety, as defined in Keeping Children Safe in Education.
- The Headteacher and Mrs Haygarth (Deputy DSL) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher/senior leaders are responsible for ensuring that the Computing lead, IT provider, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher/senior leaders will receive regular monitoring reports from the School Business Manager.
- The Headteacher/senior leaders will work with the designated technology governor and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Technology Governor who will receive regular information about online safety incidents and monitoring reports. The Technology Governor's role will include:

- Completing monitoring visits involving the Headteacher / Computing Lead (with responsibility for online safety).
- Receiving updates about any online safety incidents.
- Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended.
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards.
- Reporting to governors.

- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet with the technology governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant governing body meetings/groups.
- Report regularly to senior leadership team.
- Be responsible for receiving reports of online safety incidents and handling them, deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- Have a leading role in establishing and reviewing the school online safety policies/documents.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/pupils.
  Lliaise with school technical support, pastoral staff and support staff (as relevant).
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - Content: being exposed to illegal, inappropriate or harmful content.
    - Contact: being subjected to harmful online interaction with other users.
    - Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
    - Commerce: risks such as online gambling, inappropriate advertising, phishing etc.

Curriculum Leads

Curriculum Leads will work with the Computing Lead to develop a planned and coordinated online safety education programme.

This will be provided through:

- A discrete programme.
- PSHE and RHE programmes.
- A mapped cross-curricular programme.
- Assemblies and pastoral programmes.
- Relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They have read, understood, and signed the Staff Acceptable Use Policy and Staff Code of Conduct.
- They immediately report any suspected misuse or problem to the DSL/DDSL for investigation/action, in line with the school safeguarding procedures.
- All digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure pupils understand and follow the Online Safety Policy and Think then Click rules.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The IT Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority or other relevant body.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSL/DDSL for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in school policies.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Think then Click online safety rules and Online Safety Policy.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the "Think then Click" online safety rules.
- Publishing information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc.
- Newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to pupils in school.

Community users

Community users who access school systems as part of the wider school provision will be expected to sign the Staff Code of Conduct before being provided with access to school systems.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Dealing with unsuitable and inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school's policy restricts usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime					X

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
or comments that contain or relate to:	• Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Online gaming (non-educational)				X	
	Online shopping (not related to school)				X	
	File sharing			X		
	Use of social media			X		
	Use of messaging apps			X		
	Use of video broadcasting e.g. YouTube			X		

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff.

Reporting and responding

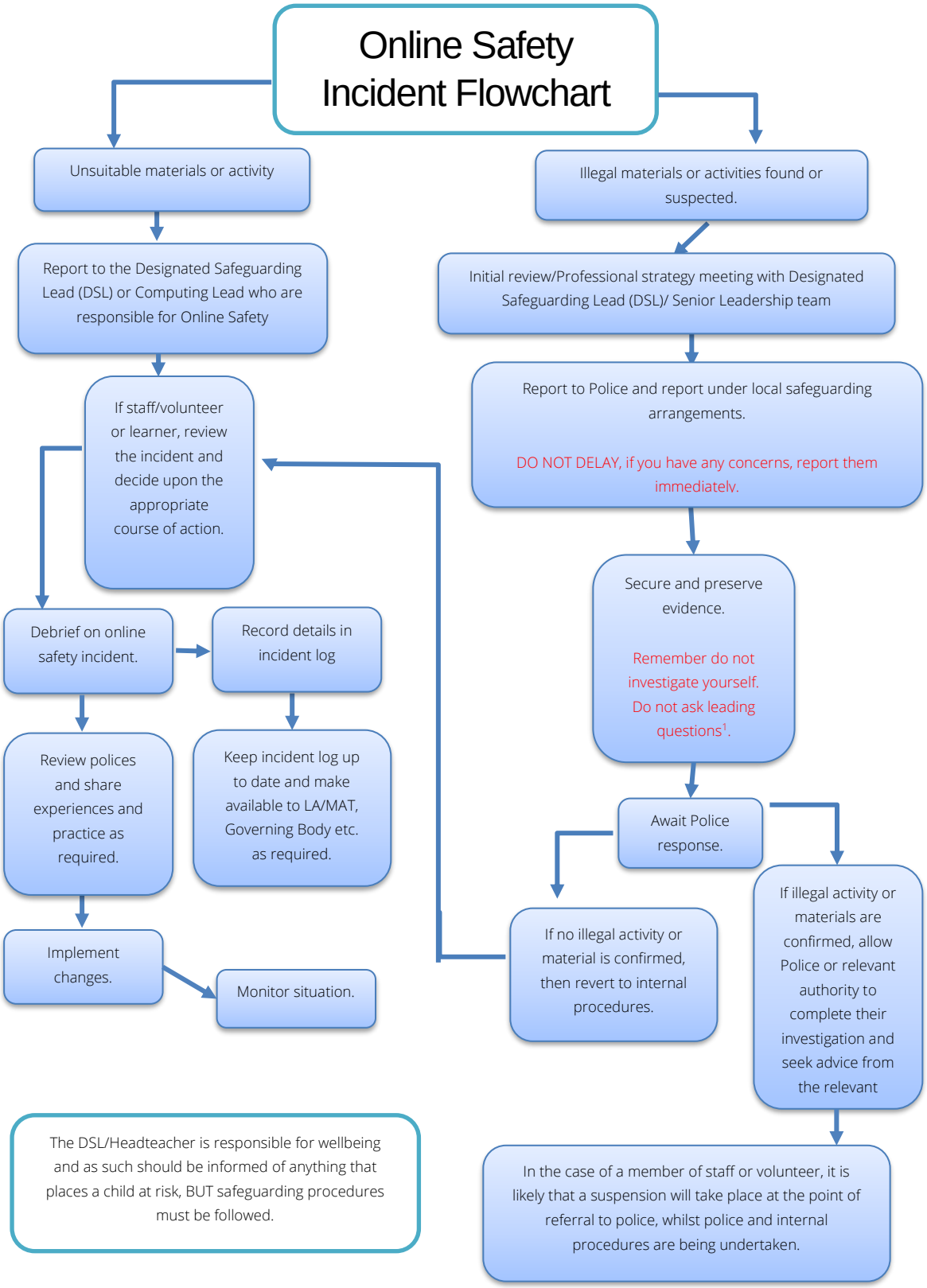
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Computing Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include: Non-consensual images, Self-generated images, Terrorism/extremism, Hate crime/ Abuse, Fraud and extortion, Harassment/stalking, Child Sexual Abuse Material (CSAM), Child Sexual Exploitation, Grooming, Extreme Pornography, Sale of illegal materials/substances, Cyber or hacking offences under the Computer Misuse Act, Copyright theft or piracy.
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident .
- Incidents should be logged on CPOMS.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Headteacher for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - pupils, through assemblies/lessons
    - parents/carers, through newsletters, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) or Computing Lead who are responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior Leadership team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in line with our Child Protection and Safeguarding Policy (where appropriate) our Positive Behaviour Policy (pupils) or Staff Behaviour Policy (Code of Conduct).

Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. At Prior Heath:

- A planned online safety curriculum for all year groups is in place.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PSHE; RHE; English etc.
- Staff use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g. for victims of abuse and SEND.
- Learners should be helped to understand the need for the Think then Click rules and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Staff/volunteers

All staff will receive training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be included in the school's annual safeguarding training for all staff.
- All new staff will receive online safety training as part of their safeguarding induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The DSL will receive regular updates through attendance at external training events, (e.g. DSL training) and by reviewing guidance documents released by relevant organisations
- The DSL will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for the designated governor for Technology. This may be offered in several ways such as:

- Attendance at training provided by the local authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Additional training will be made available to (at least) the Technology Governor. This will include:

- Cyber-security training (at least at a basic level).
- Meeting with the Headteacher/DSL to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

The school will seek to provide information and awareness to parents and carers through:

- Communication about online safety issues, curriculum activities and reporting routes.
- Letters, newsletters, website.
- High profile events / campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites/publications, e.g. www.saferinternet.org.uk/; www.childnet.com/parents-and-carers.

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The school's filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider. Every half term the DSL and DDSL complete a filtering and monitoring checking tool.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility and manage restrictions.

The overall filtering and monitoring provision is reviewed annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

Filtering & Monitoring

Filtering is managed by the school's Technology provider, Soft Egg. The SBM is alerted to breaches of the filtering policy, which are then acted upon. The DSL and DDSL undertake half-termly user level filtering.

Due to the age of the children, monitoring is mostly in the form of direct supervision by the adults in the classroom.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT.
- Password policy and procedures are implemented.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines.
- The School Business Manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Use of school devices out of school is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on a school-owned devices without the consent of the Headteacher.
- Removable media is not permitted unless approved by the SLT/IT service provider.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphones, tablets, wearable devices, notebooks/laptops or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

The Staff Code of Conduct and Acceptable Use agreements outline the expectations around the use of mobile technologies.

School staff use 'class' mobile phones to access the Tapestry online learning journal. Photographs are taken and uploaded directly to this platform of the children engaging in their learning. Photographs are deleted from these devices once uploaded. These mobile phones are kept in school.

Wearable technology (smart watches) can be worn during school day but staff should only access messages and calls during break time in the staff room. Mobile phones and smart watches are not allowed to be brought to school by pupils or taken on any school excursion.

Social media

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media.

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school and respond to these as appropriate.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- Parents will complete a "Consent to use photographic images of children" form when their child joins the school.
- Staff must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images.
- The school's Photography and Video Guidance will be shared with parents before events such as the Christmas play and sports morning.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that learners are appropriately dressed.
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- Images will be securely stored in line with the school retention policy.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Newsletters
- Email communication via ParentMail

The school website is managed/hosted by IRUN. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and Staff Code of Conduct; curating latest advice and guidance; creating an online safety page on the school website.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation. The school:

- Has a Data Protection Policy.
- Implements the data protection principles and can demonstrate that it does so.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO).
- Has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this.
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- Provides staff, parents, volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- Has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.

- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data.
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- When personal data is stored on any mobile device or removable media the:

    - Data will be password protected.
    - Device will be password protected.
    - Data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Will not transfer any school personal data to personal devices.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy is reviewed by Computing leader and governor with responsibility for Technology.