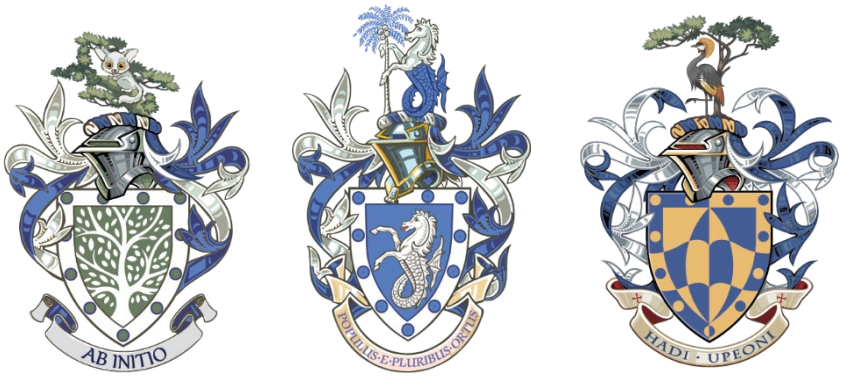


PEPONI SCHOOLS

Online Safety Policy

To be reviewed by:	Headmaster, Peponi School Head, Peponi House Head of Peponi House Kabete Kindergarten
Date of Policy:	September 2023
Review Frequency:	Annually
Review Date:	September 2024

1 About this policy

At Peponi Schools we have a strong pedagogical philosophy of linking digital learning to our pupils' curriculum to help enhance and develop learning as well as ensuring we are helping to prepare our pupils for the current world that they are living in. We aim to support our pupils in becoming flexible, fluid learners who are happy and confident to adapt to future changes. We are aware that raising the profile of digital learning in our schools means that we must have a robust strategic plan which ensures that our pupils are able to experience all that is on offer within a safe, structured environment.

This policy sets out the Peponi's safety expectations of staff, parents and pupils, in respect to the use of the Internet, e-mail, messaging systems and related technologies provided by Peponi Schools and to all Peponi users accessing these services within Peponi Schools and from home.

This policy is designed to express the Peponi Schools' philosophy and vision with regard to the Internet and digital communication in general. It aims to set general principles users should apply when using the services at Peponi, but this guidance cannot and does not attempt to cover every possible situation.

This policy is applicable to all Peponi Schools including those pupils in the Peponi Early Years Stage (EYFS) and boarders.

2 Review Procedure

There shall be ongoing opportunities for staff to discuss with the DSL and/or DDSLs any issue of E-Safety that concerns them.

The policy shall be amended if new technologies are adopted or there are changes in the regulations or guidance in any way as well as reviewed annually.

3 Introduction to online safety

Digital technology is seen as an essential resource to support teaching and learning within school, as well as playing a role in the everyday lives of our pupils. Peponi Schools need to build in the use of these technologies to prepare our young people with the skills to access lifelong learning and employment. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies young people are using both inside and outside of the classroom include:

i. Websites
ii. Virtual Learning Environments
iii. Email
iv. Instant Messaging
v. Chat Rooms
vi. Social Networking
vii. Blogs and Wikis
viii. Podcasting
ix. Video Broadcasting
x. Downloading Music
xi. Apps that have been designed for either mobiles, tablets or laptops
xii. Gaming devices with web functionality
xiii. Mobile Phones / Tablets with text, video and/or web functionality
xiv. Smart Watches
xv. Smart TVs

Whilst exciting and beneficial, both in and out of the context of education, all users need to be aware of the range of risks associated with the use of these Internet technologies.

As an integral part of the ICT/Computing curriculum, we teach students to:

i. Select, use and combine a variety of software, including internet services, on a range of digital devices to achieve stated goals, including collecting, analysing, evaluating and presenting data and information.
ii. Understand how a basic algorithm operates and to identify and fix software and algorithmic flaws, applying logical reasoning.
iii. Explain how internet search engines find and store data; use search engines effectively; exercise discernment when evaluating digital content; respect people and intellectual property; use technology responsibly, securely and safely.

At Peponi Schools, we understand the responsibility to educate our staff, parents and pupils about online safety issues; informing all stakeholders about the most up to date guidance available through staff training, parent workshops and for pupils, through assemblies and the PSHE and Computer Science/Computing curricula. Staff training occurs within the INSET timetable, and includes a focus on online elements of peer-on-peer abuse and cyberbullying, as well as consensual and non-consensual relationships on social media and ongoing review of threats to online safety, as linked to the Safeguarding Policies and Acceptable Use Policies.

This policy and the Acceptable Use Policies are inclusive of both fixed and mobile Internet technologies provided by Peponi Schools (such as PCs, laptops, tablets, webcams, digital video equipment, etc.) and any personal device of this nature that is used or can be used for work purpose and within the network.

3.1 Measures Taken

At Peponi Schools we have created a safe digital learning environment consisting of the following elements:

i. **Web Filtering/Monitoring** - Web filtering is handled by our firewall, it detects the user or device that is logged in and applies the appropriate level of filtering. The different filters are 3-11, Senior School (KS3 and KS4), Sixth Form and Staff. The categories that are blocked in each filter are decided either by the Heads of School or a member of the relevant SL. Please refer to the Appropriate Filtering and Appropriate Monitoring sections for more details.
ii. **Safesearch** - Safesearch facilities have been enabled for the major search engines and streaming media sites where possible. SSL (Secure Sockets Layer) Inspection is also enforced for pupil traffic which allows secure content to be inspected to detect search terms.
iii. **Port and Service Restrictions** - Access has been given to only essential ports and services through the firewall.
iv. **App Control** - There are several ways in which applications are restricted. The firewall has an application filter that detects specific app traffic at web level. This has been locked down to prevent pupil access to Proxy/VPN and Peer to Peer traffic. Our antivirus software also has an application filter that prevents potentially malicious application traffic running from a PC or Mac. Our group policy settings prevent apps being run from a user profile which helps prevent malware and ransomware.
v. **Mobile Device Management (MDM)** - All pupil issued devices are managed and controlled by the Peponi School's IT Department. All school devices are restricted so only approved apps can be installed. These apps are approved by the Head or Deputy Head Academic.

3.2 Appropriate Filtering

Web filtering at Peponi School is via transparent proxy on the firewall. Web filter categories are agreed by the heads of school. Requests for individual blocking or allowing of sites can be made by a member of staff and checked by a member of the IT team, or websites can be requested to be reclassified into a specific category directly with the firewall provider. If they are unsure on a particular site they will consult with the Designated Safeguarding Lead (DSL) or a Deputy Designated Safeguarding Lead (DDSL).

At Peponi Schools we have identified the below inappropriate online content to filter, recognising that no filter can guarantee to be 100% effective.

What we do:

i. Discrimination: We block the Discrimination category.
ii. Drugs / Substance abuse: We block the Drug Abuse category for all pupils.
iii. Extremism: We block the Extremist Groups category.
iv. Malware / Hacking: We block the Proxy Avoidance and Hacking category.
v. Pornography: We block the Pornography category.
vi. Piracy and copyright theft: We block the Plagiarism category for all pupils.
vii. Self Harm: There is no specific category for Self Harm in the firewall but all abuse categories are blocked for all pupils.
viii. Violence: We block the Explicit Violence category.

3.3 Appropriate Monitoring

Physical Monitoring - Pupils in Kindergarten to Year 8 in the 3-13 environment are closely supervised and do not have access to devices without a member of staff present.

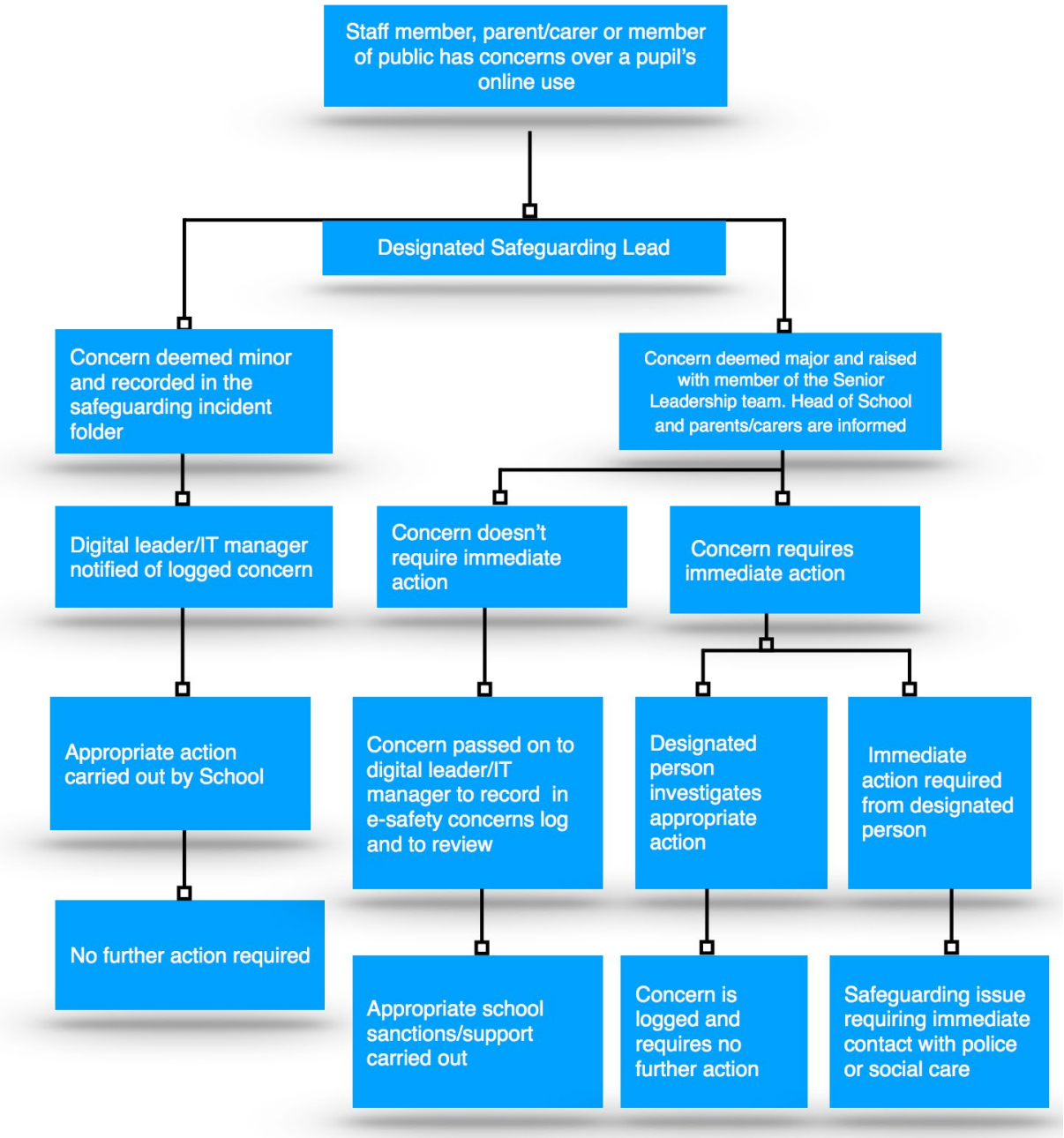
Internet and Email Monitoring - All Internet and school email activity that goes through Peponi School systems is logged. Reports of web activity (including search terms) are sent at regular intervals to the Designated Safeguarding Lead (DSL) and the appropriate Deputy Designated Safeguarding Lead (DDSL). Where pupils share devices, a device search terms report is also sent. The reports contain a vast amount of information and detail so it is not feasible for all activity to be checked. However, if there is a particular concern or issue raised about a pupil, their web activity (using the reports as reference) and email history will be analysed. Random spot checks of users in the reports may be done for safeguarding and pedagogical reasons.

Active Monitoring - In order to actively identify “at risk” pupils whilst at school, potentially preventing a safeguarding incident, email alerting has been set up. This means that if pupils search for a particular keyword, the DSL or appropriate DDSL will be alerted via email. They will then be able to assess whether further investigation is required. They will be able to use the web activity reports mentioned above as a reference to check for any further online behaviour that is cause for concern. The keywords list is subject to change and determined by the Safeguarding Team with guidance from various industry sources. In addition to the keywords, email alerts are sent to the DSL and appropriate DDSL when a pupil attempts to access a website in high risk categories. Due to the high volume of alerts and the fact they could come in outside of school and term times, it is not feasible to expect an immediate response to them.

4 Roles and responsibilities

The Headteachers and Board of Directors have the ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of Peponi School community have been made aware of who the DSL and the DDSLs are. Any online safety concerns will be logged through the Peponi Schools’ reporting systems, and they will be actioned as necessary.

Flowchart showing action to be taken in the event of concerns over a pupil's online use



4.1 Peponi School's Responsibility

As stated earlier, online safety covers a wider scope than just the Internet. Peponi School includes the following in the Online Safety Policy:

i. DSL and DDSLs can request and access support and advice from outside agencies including CPAN
ii. The DSL and DDSLs will maintain the Online Safety Policy, manage online safety training and keep abreast of local and national E-Safety awareness campaigns.
iii. Peponi Schools shall update the online safety policy as required and review the policy annually to ensure that it is current and considers any emerging technologies.

iv. The Peponi Schools' IT Managers shall consult with the DSL and where appropriate the Heads of School to audit the Peponi Schools' filtering systems to ensure that inappropriate website categories are blocked.
v. Peponi Schools will ensure that pupils and staff are adhering to the policy, by logging any incidents of possible misuse, and ensuring that these are investigated, where appropriate, by a member of the relevant Senior Leadership Team or the DSL or DDSL.
vi. Peponi Schools shall consider online safety whenever members of its community are using the Internet and ensure that every pupil has been educated about safe and responsible use.
vii. Pupils and staff need to know how to minimise online risks and how to report a problem, if in school or at home.
viii. All staff shall agree to and sign the Technology Acceptable Use Policy.

4.2 Implementation

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. Online safety awareness is an essential element of all staff and volunteer induction. Training is therefore delivered to cover the following points:

i. Pupils should be reminded of their responsibilities whenever they are using the Internet, both in terms of the Acceptable Use Policy, in navigating social media and the internet generally safely themselves, and in how to recognise and report cyberbullying and peer-on-peer abuse directed at themselves or others.
ii. Ensuring all staff, pupils and parents know how to report an incident of concern regarding Internet use, as well as what specific concerns may look like in a digital context.
iii. A member of the relevant SLT approves the Peponi Schools' web filtering configuration.

4.3 Responsibilities and Expectations of Peponi Staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss online safety issues with pupils. Advice and training for staff shall be incorporated into Child Protection Training which all staff must complete during their induction to Peponi Schools and every 3 years. All staff must be signed off to state that they have attended this training.

There will be additional online safety training provided through twilight training sessions run after school and on whole staff INSET days. New and relevant information, which needs to be brought to the attention of all staff immediately, will also be incorporated into safeguarding briefings.

All staff shall sign an Acceptable Use Policy for staff on appointment and re-sign a new policy if any significant amendments are made. Staff know and accept that Peponi Schools can monitor network and Internet use to help ensure staff and pupil safety.

The IT Department is responsible for the web filtering on all Peponi Schools' devices whilst onsite.

If a member of staff suspects a pupil of viewing or using inappropriate or illegal content, it must be reported to the DSL or DDSL. Staff must be aware of dangers to themselves in managing ICT use; for instance, if staff view inappropriate images to investigate their source, this needs to be reported to the DSL or DDSL immediately.

Any allegation of inappropriate behaviour by staff must be reported to the relevant SLT and investigated with care. Advice should be sought from the DSL.

Email, text messaging, Social Media and Instant Messaging (IM) all provide additional channels of communication between staff, parents and pupils. Inappropriate behaviour can occur and communications can be misinterpreted. When sending parents or pupils an email, staff must only use the Peponi Schools' mailing systems. Staff must not give out their own personal contact details. Staff must never send or accept texts or images that could be viewed as inappropriate. If a member of staff receives content that is offensive

in any way they need to notify a DSL so that the matter can be investigated further. Contact with pupils and parents must be through Peponi devices and systems only.

In limited circumstances, it may be appropriate for staff to use a personal mobile phone for work purposes. Where possible this should always be agreed with a DSL in advance. Such circumstances include:

i. Emergency evacuations
ii. Parental contact in an emergency (mobile phones setting that allow for the number not to be identified should be used)

It is essential that staff do not accept pupils or parents as friends or "follow" them on social media websites – until there is no longer any professional responsibility for the pupil (when the pupil has left Peponi Schools). Consideration should be given to the age of the pupil at the time of leaving and caution exercised even when there is no professional responsibility. Staff must ensure their personal social media accounts do not risk the reputation of themselves or Peponi Schools and suitable privacy settings are applied where necessary.

Internet chat rooms and online forums pose risks for staff and pupils. Whilst they can offer many positive experiences, there is widespread concern about their potential abuse by paedophiles attempting to groom new victims. The advice is that staff should not use unregulated chat rooms for children and should be aware that it is impossible to determine the age of any participant in these environments. They must not enter into any newsgroups, chat or interactive messaging discussion areas that are not primarily for education professionals without consulting a member of the relevant SLT.

Staff should be aware that pupils may be subject to child-on-child abuse or cyberbullying via electronic methods of communication both in and out of school. If a pupil informs staff that this is happening, staff have an obligation to report this to the DSL/DDSL. Staff must not investigate an issue themselves or ask a pupil to investigate.

Protection of Peponi accounts and data is vital. Reference should be made to the Technology Acceptable Use policy for staff for further information.

Authorised images taken of pupils using a Peponi device shall be removed from it and stored securely on Peponi systems, and not kept longer than necessary. Staff need to take particular care with sharing features to make sure images are not synced or shared to other unsecured or unauthorised devices or persons. Location settings should be appropriately configured to keep the location of staff and pupils private.

School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policies.

Related Policies:

i. Risk Assessment Policy for Pupil Welfare
ii. Safeguarding and Child Protection Policy