THE HERMITAGE SCHOOLS

Inspire, Learn, Achieve

Online Safety Policy

Persons Responsible:	Computing Leader & Behaviour and Welfare Leader
Date Adopted:	July 2010
Date of last review:	Summer Term 2025
Date of next review:	Summer Term 2026

Policy Links

- ICT Policy
- ICT Acceptable Use Policy for staff
- Social Media Policy
- Rules for Responsible Internet Use for parents and pupils
- Child Protection & Safeguarding Policy
- Behaviour & Exclusions Policy
- Anti-Bullying Policy
- PSHE and Citizenship Policy
- Mobile Phone Policy

Rationale

Our Online Safety Policy has been written by the schools, building on best practice and government guidance. The Policy is an extension of our ICT Acceptable Use Policy (AUP) for staff and our Code of Conduct for ICT for parents/carers and children. It is aimed at ensuring the safety and well-being of all pupils when accessing ICT based learning. The policy builds upon government guidance, to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The internet is an essential element in 21st century life for education, business and social interaction. The schools have a duty to provide students with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The schools will ensure that all members of their community are aware of the Online Safety Policy and the implications for the individual. Online safety depends on staff, governors, parents/carers and, where appropriate, the pupils themselves taking responsibility for the use of the internet and other communication technologies.

Our vision for online safety

The Schools provide a diverse, balanced and relevant approach to the use of technology:

- Through a variety of media, the children are encouraged to maximise the benefits and opportunities that technology has to offer.
- The schools aim to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
- The children are increasingly being equipped with the skills and knowledge to use technology appropriately and responsibly.
- The schools aim to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.
- The users in the school community understand why there is a need for an Online Safety policy.

Using this policy

The Online Safety Policy covers the use of all technology which can access the schools' network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand-held games consoles used on the school site.

The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff/pupil.

The Online Safety Leaders are responsible, along with the Executive Headteacher, Senior Leadership Team and Governors, for taking the lead in embedding effective online safety practices into the culture of the schools.

As online safety is considered a safeguarding issue, the Online Safety Leader in each school is also a Designated Safeguarding Lead (DSL) and member of the Senior Leadership Team.

The Online Safety Leader in each school is responsible for promoting an awareness and commitment to Online Safety throughout the school by:

- Being the first point of contact in school on all online safety matters.
- Creating and maintaining online safety policies and procedures.
- Developing an understanding of current online safety issues, guidance and appropriate legislation.
- Ensuring all members of staff receive an appropriate level of training in online safety issues.
- Ensuring that online safety education is embedded across the curriculum.
- Ensuring that online safety is promoted to parents/carers and in response to current events or issues.
- Liaising with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitoring and reporting on online safety issues to the Senior Leadership Team and governors as appropriate.
- Ensuring that an online safety incident log is kept up to date.

Managing access and security

- The schools will provide managed internet access to staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The schools will use a recognised internet service provider or regional broadband consortium. Internet access in the schools is currently provided via wired and wireless broadband from RM Education. Filtering appropriate to the age of the pupils is provided as part of this link. The entire ICT system operates behind a secure firewall to prevent external programs and systems gaining access. This virus protection system is automatically updated. School internet access is filtered using HTTPS decrypt and inspect.
- Pupil access to the internet will be by adult demonstration or directly supervised access to specific, approved on-line materials. Instruction in responsible and safe use by pupils will precede internet access.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The schools will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Staff responsibilities

- All members of staff including teachers, teaching assistants and support staff, will be provided with access to a copy of the school Online Safety Policy, ICT Acceptable Use Policy and Social Media Policy. All staff are required to sign to say that they have received, read, understood and agree to comply with the ICT Acceptable Use Policy before using any internet resource in school. Supply staff will be provided with a copy of an abbreviated ICT Acceptable Use Policy which they will be asked to sign before using any internet resource in school.
- All staff will be made aware that internet traffic can be monitored and traced to the individual user and professional conduct is essential. Staff development in safe and responsible internet use will be provided as part of the schools' continuing professional development programme.
- The schools will keep an up-to-date record of all staff and pupils who are granted internet access.
- The Senior Leadership Teams, including the Online Safety Leaders, will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

Internet Use

- The schools will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- All communication between staff and pupils or families will take place using school equipment and/or school accounts.
- Pupils will be advised not to give out personal details or information which may identify them or their location.

Teaching and Learning

- As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the internet, as well as made aware of what is not acceptable.
- All pupils will be given clear objectives when using the internet. Where internet activities are part of the curriculum, they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through online activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the schools.

- Curriculum activities that involve the use of the internet for gathering information and resources will develop pupil skills in locating and evaluating materials. Pupils will be taught how to validate materials they read before accepting their accuracy. Other techniques for research will be developed through the use of a limited group of school approved sites. Where materials gathered from the internet are used by pupils in their own work, they will be taught to acknowledge the source of information used. The schools will ensure that the use of internet materials by staff and pupils complies with copyright law.
- Emerging technologies will be examined for educational benefit and any risks considered by the Senior Leadership Teams, the Online Safety Leaders and the Computing Leaders before use in the schools is allowed.

Email

- Pupils and staff may only use authorised, school-controlled email accounts on the schools' IT systems.
- Staff passwords, either for logins or email accounts, should never be shared with pupils or other members of staff.
- Curriculum activities that involve the use of email must only take place via a school email address or from within the learning platform.
- Incoming emails should be treated as suspicious and attachments not opened unless the sender is known.
- The school will consider how email from pupils to external bodies is presented and controlled.
- The use of individual pupil personal accounts will not be permitted through the school system and must not be accessed.

Published content, e.g. the schools' websites and social media accounts

- The contact details will be the schools' addresses, emails and telephone numbers. Staff or pupils' personal information will not be published.
- The Executive Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs of pupils or pupil names are published on the websites or other social media sites controlled by the schools.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the schools' websites or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. Only first names of pupils will be published.

Use of social media including the schools' learning platforms

- The schools will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Access to video and multimedia content from unregulated sites will be prohibited at school and blocked by the systems' firewalls. Any multimedia content brought in by staff for teaching and learning purposes must be checked for appropriate content before being used in lessons. If there is any doubt as to whether the content is age appropriate or not, it should be referred to and checked by the Online Safety Leader or a DSL before being used in lessons.
- Use of video services such as Zoom, Microsoft Teams and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- The use of online chat rooms, instant messaging services and text messaging will not be allowed in the school community, as these technologies cannot be supervised or monitored in a way that

will guarantee the online safety of the pupils. Furthermore, there are no explicit learning outcomes from using these technologies within the school community.
- Staff and pupils should ensure that their online activity, both in school and out, takes into account the feelings of others and is appropriate for their situation as a member of the schools' communities.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone that they have met online. If contact is made with a pupil from an external source through the internet, the pupil should inform a member of staff immediately.
- The school has a separate social media policy.

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the Online Safety Policy and the relevant AUP.
- Staff must not store images of pupils or pupils' personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Use of mobile phones

- The use or carrying of mobile phones by pupils will not be permitted during formal school time or on school trips. This is due to the expensive cost of mobile phones and the possibility of the school being liable if a phone was lost, stolen or broken on school premises. Secondly, these devices could be used to send inappropriate or offensive or abusive material.
- If for any reason a parent/carer deems it necessary for a child to bring a mobile phone to school, the parent/carer must have prearranged this with the school in advance and the phone must be handed over to the class teacher, by the child, at the start of the day and be collected by the child at the end of the day. However, the schools can take no responsibility for mobile phones that are brought into school.
- Staff mobile phones should be on silent during the school day and must not be available for children to access.
- The schools have a separate mobile phone policy.

Protecting personal data

- The schools have a separate Data Protection Policy, written in accordance with the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

Policy Decisions

Authorising access:

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign to say they have understood and agree to comply with the 'Staff AUP' before accessing the schools' IT systems.
- The schools will maintain a current record of all staff and pupils who are granted access to their IT systems.
- Pupil access to the internet will be with teacher permission with increasing levels of autonomy.
- People not employed by the schools must read and sign the 'AUP for Visitors' before being given access to the internet via school equipment.
- A consent form, which covers permission to access the internet, will be issued to parents and carers when their child joins the schools. This will contain guidelines and details of using the internet responsibly. Parents/carers will be required to sign the consent form. The signed consent form must be returned to the school for pupil access to the internet to be permitted.

Pupils will be informed that internet use will be monitored. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to.

- All classes will be taught and reminded of the schools' rules involving internet use and online safety. This should take place in the first Computing lesson of the year. Reminders of the Pupil Rules regarding internet and ICT use should be displayed in all rooms which have access to a computer.

Assessing risks

- Some material available on the internet is unsuitable for pupils. Methods to identify, assess and minimise risks will be reviewed regularly. The schools will take all reasonable precautions to ensure that pupils access only appropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the schools nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.
- Where unsuitable content is encountered, staff and pupils should follow the school procedures for such events. Unsuitable URL addresses will be reported through the school office to the LA broadband technical support team. Pupils must report unsuitable material, including email content, immediately to a teacher. The teacher will then ensure that the appropriate reporting procedures are followed. Parents will be informed of such incidents sensitively to avoid undue distress.

Handling online safety complaints

- Complaints of internet misuse will be dealt with according to the Behaviour and Wellbeing Policy.
- Complaints of a child protection nature must be dealt with in accordance with schools' child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' Behaviour and Wellbeing Policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed the school's 'AUP for Visitors', so it is expected that their use will be in accordance with the schools' Online Safety Policy.

Misuse of internet

- Where incidents occur due to non-compliance with the Online Safety Policy, these will be reported to a member of the Senior Leadership Team. Any issues relating to staff misuse must be referred to the Executive Headteacher. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Should it become necessary to prohibit the use of internet resources for a pupil, then parents/carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe internet use at home.