Swiss Gardens Primary School

Swiss Gardens
Shoreham-by-Sea
West Sussex BN43 5WH

POLICY · STATUTORY & LEGAL

Online Safety Policy

Adopted July 2026 · next review July 2028

ABOUT THIS POLICY

How we keep children safe online, in school and at home — covering filtering, monitoring, what we teach, and what to do if something goes wrong.

The full policy follows from the next page.

Swiss Gardens Primary School		
Policy:	**Online safety Policy**	
Policy date:	July 2026	
Review date:	July 2028	
Person responsible	SLT/ governors	

INTRODUCTION

The internet plays a significant role in raising standards, the promotion of pupil achievement and the support of the professional duties of staff. We recognise the internet is an essential element in modern education, business and social interaction. Our school has a duty to provide students with safe, quality internet access as part of their learning experience.

E-safety depends on effective practice in each of the following areas:

- Education for responsible use of ICT by staff and pupils.
- A comprehensive and fully implemented E Safety Policy.
- Secure, filtered broadband internet access.
- An effective and reliable school network and ICT facilities

MANAGING INFORMATION SYSTEMS

How will information systems security be maintained?

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be guided by the Local Authority.
- Ensure the security and safety of the wireless network system.
- School or LA data will not be stored on personal devices.

How will email be managed?

- Pupils may only use approved email accounts on the school system and will only do so under supervision and all communications will be monitored.
- In any external email communication pupils must not reveal personal details, those of others, or arrange to meet anyone without specific permission.
- External email will normally only be provided through whole-class or group emails.
- The forwarding of chain letters, emails or messages is not permitted under any circumstances.
- Incoming email should be treated as suspicious and no attachments opened unless the sender is known.
- Access to external personal email accounts may be blocked on school premises.
- Pupils are provided with a secure and closed system – school's Onedrive – through which internet and communication skills, including email, may be rehearsed.

How will published content and the school website be managed?

- Staff and pupil personal contact details information will not be published. Only school contact details will be made available.
- The Headteacher has overall editorial responsibility for the website and will ensure that information is accurate, appropriate and compliant with legal obligations.

Can pupil's images or work be published?

Photographs that include pupils will only be published if all pupils in the image are covered by parental permission to do so. Pupils' full names will not be published in association with photographs without parental permission

How will social networking and personal publishing be managed?

- Social Network sites and newsgroups will be filtered unless a specific use is approved.
- Pupils will be advised never to give out their personal details of any kind which may identify them, their friends or location when using social network resources out of school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of potential dangers for pupils.

How will filtering be managed?

- The school work with ENTRUST to ensure systems to pupils are reliable, reviewed and improved.
- A wide range of sites are filtered to protect users from inappropriate and illegal material. Some sites, filtered automatically, but of educational value may be by released from filtering on request.
- If staff or pupils come across unsuitable online materials, the site must be reported to the e-safety leader (Headteacher).

How will video conferencing be managed?

- Video conferencing should always be via the school's broadband network to ensure quality of service and security – it must not be via personal devices e.g. Smart Phones.
- Pupils do not routinely make video calls unless in a specific teaching circumstance and they must ask permission from the supervising teacher before making or answering a video conference call. Pupil conferencing will only be used for teacher lead activities with groups or classes
- All video conferencing and webcam use will be under supervision appropriate the primary aged pupils.

How will emerging technologies be managed?

- Emerging technology including applications and software will be examined for educational benefit and potential risks assessed before use in school. Any requests to employ such resources and technologies should be made to the esafety leader (Headteacher).

How is out of hours communication between staff and pupils be managed?
The school does not currently use an apps that enable out of school hours

May staff use personal devices?

- Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present routes to undesirable materials and communication – these should not be used by pupils in school.
- Pupil should not be given access to personal devices owned by staff or other adults.
- Staff may use personal devices for private purposes but must not access any inappropriate material via these devices or use personal phones etc. to send or receive calls during lessons or when responsible for the supervision of children, without prior permission (in exceptional and occasional circumstances) from a member of the SLT.
- Staff personal devices should not be in view of children at any time

How will personal data be protected?
Personal data will be recorded, processed, transferred and made available only in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

POLICY DECISION

How will internet access be authorised?

- All staff are required to read and sign the Acceptable Use Policy for ICT before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- In EYFS and Key Stage 1, internet access is normally by adult demonstration or with appropriately supervised access to specific, approved, online materials and activities.
- Parents are asked to sign and return an internet use consent form before their children are allowed access to the internet and communication resources.

How will risks be assessed?

The school will take all reasonable precautions to prevent access to inappropriate material. However due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor West Sussex County Council can accept liability for any material accessed, or any consequences of internet access. The school will, from time to time, audit ICT use to monitor the effectiveness of this online safety Policy.

How will e-safety complaints be handled?

- Complaints regarding the misuse of the internet will be dealt with by a member of the Senior Leadership Team (SLT).
- Any complaints about staff misuse must be referred to the Headteacher or, if the complaint is about the Headteacher, to the Chair of Governors.
- Complaints related to Child Protection will be dealt with in accordance with the Safeguarding Policy and the Designated Safeguarding Lead for Child Protection (Headteacher) or Deputy DSL will be informed immediately.

How is the internet used across the community?

- The school will liaise, as appropriate, with local organisations to establish a common approach to e-safety if required.
- The school will be sensitive to internet related issues experienced by pupils out of school and will offer appropriate advice and support as necessary.

<u>COMMUNICATION POLICY</u>

How is the e-safety policy introduced to pupils?

- E-safety rules will be displayed where computers are used and pupils will be made aware of them at regular intervals.
- Pupils will be informed that network and internet use will be monitored and followed up if necessary.
- E-safety training is incorporated in ICT and Computing teaching.

How is the e-safety policy discussed with staff?

All staff will be made aware of the school e-safety policy, its importance will be explained and they will be required to acknowledge that they have read and understood the policy.
Staff will use a child friendly, safe search engine when accessing the web with pupils.

How will the support of carers' and parents' be enlisted?

Parents' and carers' attention will be drawn to the school e-safety policy in newsletters and via the school website. The school will, as necessary, make training, advice and information, regarding e-safety, available to parents and carers.

The school will ask all new parents to sign the home school agreement and the internet access agreement when they register their child with the school.