

Godstowe

School Policy

Online Safety

Reviewed
September
2025

Godstowe aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1. Introduction and overview

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. This will include considering how online safety is reflected in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the Designated Safeguarding Lead and any parental engagement. Godstowe's whole school approach safeguards and protects the students and staff and helps them to work safely and responsibly with the internet and other communication technologies.

Pupils in Years six, seven and eight are allowed to use a 1:1 school managed device in lessons. The school network is carefully monitored and locked down to stop access to undesirable sites. However many of these children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children could, whilst at school, sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. Godstowe has carefully considered how this is managed on their premises and reflected in the Mobile and Smart Technology policy and the Safeguarding policy.

Godstowe sets clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use. There are clear reporting mechanisms to deal with online abuse such as bullying. Godstowe ensures that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of the school community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of the school's ICT systems.

Communication of the policy

The policy will be communicated to the school community in the following ways:

- Displayed on the school website

- It forms part of the induction procedure
- Acceptable use agreements are discussed with and signed by students at the start of each year
- Acceptable use agreements are issued to the whole school community, usually upon entry to the school
- Acceptable use agreements are signed and held in student planners in Main School (Years 3 to 8) and in student files in Lodge (Years 1 and 2)
- Electronic copies of staff agreements are maintained

Responding to complaints

- The school will take all reasonable precautions to ensure online safety. However, due to the very nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of internet access.
- Our DSL is the first point of contact for any complaint. Any complaint about staff misuse will be referred to the Headmistress.
- Complaints that relate to online bullying will be dealt with in line with the Anti-Bullying Policy.

Review and Monitoring

The school's DSL is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and online safety issues which arise within the school.

This policy has been developed in consultation with the Head of Digital Learning and approved by the Senior Leadership Team. Staff will be informed of any updates or amendments to it.

2. Education and Curriculum

Student online safety curriculum

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying); and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your children, pupils, or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Online/Remote learning

Godstowe has appropriate filters and monitoring systems in place on the school network to safeguard their systems, staff and learners. These are regularly checked for the effectiveness of these procedures to keep up with evolving cyber-crime technologies.

The school has a clear, progressive online safety education programme primarily as part of the Computing curriculum / PSHE curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy
- Acceptable online behaviour
- Understanding of online risks
- Privacy and security
- Reporting concerns

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Agreement signed by every student.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.
- Provide staff and governor training via the most appropriate online provider.
- Staff understand the requirements of the GDPR in terms of sending and receiving sensitive personal information.
- Regular updates are circulated to staff on online safety issues and the school's online safety education programme.
- Information and guidance on the Safeguarding policy and the school's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. As part of our ongoing support to parents with Online Safety, they all have access to our subscription with National Online Safety. To further support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements (pupils) to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face-to-face sessions in school.
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

3. Conduct and Incident Management

Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Agreements they have signed. They should understand the consequences of misuse, or accessing inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively. The school actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about students.

4. Managing the ICT Infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by Google Safe Search. There is a clear ticketing process in place to deal with requests for filtering changes.
- The school allows different filtering levels for different ages/stages and different groups of users – staff/students.
- The school regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for staff to report any technical incident or security breach. Students are reminded to tell a member of staff if they have any concerns.
- Security measures are in place by means of LIBRA and SOPHOS XG Firewall and Endpoint to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are monitored regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Staff are fully aware that personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured using Google Drive.
- The DSL is alerted to any E Safety triggers via Net support and GoGuardian programmes. This allows for real-time monitoring and action.

5. Data

The school has a Data Protection Policy that is regularly reviewed and updated.

6. Equipment and Digital Content

Use of Mobile Technologies

Personal mobile phones and mobile devices brought to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal mobile phones or mobile devices.

Pupil Use

Girls in Years 6-8 are able to use 1:1 school managed devices in lessons. These use the school internet which prevents pupils accessing unacceptable sites. Parents need to insure these devices before they allow their daughters to bring them into school.

Pupils should not bring mobile phones or watches that connect to the internet into school unless otherwise agreed by the Headmistress. Any device brought into school without permission will be confiscated. Please see the Mobile Phone and Smart Technology Use policy for full details of usage at Godstowe.

Staff Use

Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team. Staff should not use their own devices, such as mobile phones or cameras to take photos or videos of students. All recordings and photographs of children should be taken on a school device.

Digital images and video

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission. Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school. Please see the Images: Photography of Children policy for more details.