



Gosfield School

Acceptable Use of Mobile Phones and Other Electronic Devices

Whole School Policy, including EYFS

This policy relates to the use of technology, including:

- Office 365 (including email)
- internet access
- social networking, messaging, generative AI and interactive websites/applications (for example Facebook, TikTok, Instagram, WhatsApp, Snapchat, Character.AI, ChatGPT and Grok). This list is not exhaustive and will change as new services emerge
- instant messaging, chat rooms, blogs and message boards
- gaming sites
- smartphones
- smartwatches
- smartglasses
- mobile phones with the capability for recording and/or storing still or moving images
- webcams, video hosting sites such as YouTube
- laptop, tablet and desktop computers
-
- games consoles
- other photographic or electronic equipment

It applies to the use of any of the above on school premises and also any use, whether on or off school premises, which affects the welfare of other students or where the culture or reputation of the School are put at risk. The policy applies to both students and staff.

THE ROLE OF TECHNOLOGY IN OUR STUDENTS' LIVES

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles and portable consoles, together with smartphones, provide unlimited access to the internet, to SMS messages, Forums, to FaceTime, Microsoft Teams (video calls, via web cameras built into computers, smart devices), to wikis (collaborative web pages), chat rooms, social networking sites and video sharing sites.

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Gosfield School to teach our students how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment. Specific information and teaching sessions are organised as part of the School's PSHEE programme.

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

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news including disinformation, misinformation and conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism and hate crimes.

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, harass or exploit them for sexual, criminal, financial or other purposes.

conduct: 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 deepfakes or videos with the increased risks from AI).

commerce: risks such as online gambling, inappropriate advertising, phishing, fraud and financial scams. Suspected phishing or cyber-security incidents must be reported to the IT Network Manager; safeguarding concerns must be reported to the DSL in line with the School safeguarding procedures.

STUDENT USE OF MOBILE PHONES AND OTHER ELECTRONIC DEVICES

Whilst it is recognised that parents may wish to contact their children and vice versa, Gosfield School operates as a mobile-phone-free environment throughout the school day in line with statutory DfE guidance from 1 September 2026. Pupils should not have access to or use mobile phones or other smart technology during lessons, movement between lessons, breaktimes or lunchtime, except where an agreed individual exception or reasonable adjustment applies. Pupils needing to make a call can do so through the main school office; parents should contact the School office if they need a message passed to a pupil.

On entering the school grounds all students in Years 7-11 must place their phone in their bag, this should be switched off. They may only be used during the day with the express permission of a member of staff. All Senior students' phones must be placed in a pouch and placed in their school bag or locker, it should not be seen or heard during the school day please see our Mobile Phone Policy. All Prep pupils' phones should be handed into their class teachers.

Sixth form students are allowed to carry mobile phones and may use them discretely in designated areas.

- If mobile phones are brought to school, parents and students must be aware that Gosfield School takes no responsibility for the loss or damage to the device.
- In the case of an emergency, students may be given permission to use their mobile phones by a member of staff.
- Students must not use their phone to access inappropriate material using 3G/4G/5G networks.
- Students must not use their phone as a "Personal Hotspot" In order to get around school filtering.

The use of other electronic devices, such as portable games consoles, electronic readers and personal cameras, is not allowed unless authorised by a member of staff. School-issued 1:1 iPads are provided for learning and may be used only in accordance with teacher direction, this policy and the Pupil ICT

Acceptable Use Policy. Each iPad remains the property of Gosfield School, is assigned to an individual user and is remotely managed through Jamf. The School applies its configuration, security, filtering and safeguarding policies to these devices. Student activity on school-managed iPads may be monitored using Atvion StudentKeeper (formerly Impero) for safeguarding, online-safety and acceptable-use purposes. Users must not remove management profiles, disable monitoring or filtering, share the device with another user, or attempt to bypass school controls. Camera, microphone, screen-recording, AirDrop and messaging functions may be used only when expressly authorised for a school activity and with appropriate permission.

Students must be aware that the use of their own cameras, voice recording, or social media messaging in any form is not allowed on the school site and that the following sanctions will apply.

SANCTIONS

In the first instance, this will be for a period of seven school days. The phone will be stored in a lockable cupboard in the main school office. It will be returned to the student at the end of this period.

- If a student has a phone confiscated a second time, it will be taken for two weeks, and the parent/ carer of the student will be asked to collect it. A meeting with the parent/ carer will take place to discuss further action should it happen again; this may result in the student being excluded for a set period.
- Parents should be aware the school does not accept any liability for loss or damage for a phone brought into school including during confiscation.
- Staff will consider whether the confiscation is proportionate and consider any special circumstances relevant to the case. The school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- Where there may be a related behaviour issue for example bullying or safeguarding the school leaders will be allowed access to the mobile phone to proceed with an investigation, this is supported by the DFE guidance.

The School has robust monitoring and filtering systems in place :

Filtering is preventative and monitoring is reactive. The School reviews its filtering and monitoring provision at least annually and when significant technology changes are introduced. Access to monitoring alerts and reports is restricted to authorised, appropriately trained staff and concerns are escalated to the DSL where safeguarding thresholds are met.

These measures will:

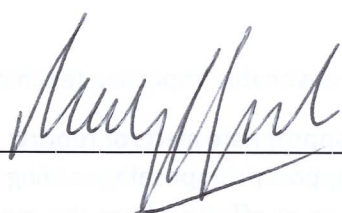
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
 - identify users and devices where possible, generate appropriate alerts or reports about potentially harmful, inappropriate or unauthorised activity, and support prompt safeguarding follow-up.
- Monitoring may include school-managed devices used on or off site where the monitoring service is configured to operate.

STAFF USE OF MOBILE PHONES AND OTHER ELECTRONIC DEVICES

- Staff should refrain from using their mobile phone when in charge of a class and use school issued trip phones or devices where possible to perform digital tasks, such as taking the register and photos. To set an example to students' staff should not use their phone during a lesson for checking personal messages or social media platforms. EYFS and Nursery staff should not have access to a phone or other technology, smartwatch, whilst supervising pupils. They can only use their phone/ device/ smartwatch in designated safe spaces away from the children, this is to protect the staff and the pupils. If staff do take photos on their personal

devices, these should be uploaded as quickly as possible to the School OneDrive account and deleted from their device as soon as possible.

- No members of staff are allowed to access their phone in the presence of EYFS and Nursery pupils, this also applies to common areas of the school like the dining hall or corridors.
- School-owned staff and student desktops, laptops and iPads may use Smoothwall and Ativion EducationPro (Education Pro) monitoring and filtering. This is used to support safeguarding, online safety, cyber security and acceptable use for school users and clients using School systems. School-owned devices and the data held on them remain the property of Gosfield School. The School reserves the right to monitor use of its systems and school-owned devices where lawful, necessary and proportionate, including for safeguarding investigations, security and policy compliance.

Signed  Date 1/9/2026
Principal

Date of next review: September 2027