Internet and ICT Policy

September 2025

To be renewed September 2028

This policy applies to pupils and staff – where there are any differences in what is permitted for each group, this will be clearly stated.

E-SAFETY AND ONLINE BEHAVIOUR – OUR APPROACH

The school adopts an approach to online safety which seeks to reduce risk as far as possible without depriving pupils of the benefits of technology.

The pupils receive education about all aspects of keeping themselves safe online and appropriate online behaviour. (See CCCS Acceptable Use Policy)

The breadth of issues classified within online safety is considerable, but is categorised in Keeping Children Safe in Education into four main areas of risk:

> **content:** being exposed to illegal, inappropriate or harmful material
>
> **contact:** being subjected to harmful online interaction with other users
>
> **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
>
> **commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The School does all it reasonably can to limit the pupil's exposure to the above risks in school and pupils also receive guidance on the safe use of the internet and are educated about the risk of online harm (including anti-bullying) primarily through their PSHE and Computing lessons.

Cyber-bullying by pupils, via texts, direct messages, social media or email, will be treated as seriously as any other type of bullying and will be managed through the school's anti-bullying policy and procedures.

If staff suspect that a pupil may be at risk of or suffering from online harm, they must report this to the DSL following procedures set out in this policy.

If a member of staff becomes aware of an incident involving inappropriate material (whether this has taken place in or out of school) they should follow the safeguarding procedures and report it to the DSL immediately. The member of staff should confiscate the device involved. Staff should not view images, delete images or look for further images. They should not copy or print images, nor forward images by email or any other electronic means.

Parents will be informed at an early stage of inappropriate online behaviour, unless there is reason to believe that involving parents would put the pupil at risk of harm. If there is concern a young person has been harmed or is at risk of harm, a referral will be made to Children's Services.

FILTERING

The school uses the filtering provided by Schools Broadband, which is set to a high level of sensitivity to limit the content pupils are able to access on the Internet. The settings for staff Internet access are set to a different level, but staff are still only able to access legal content which is appropriate for a school setting.

If a pupil or member of staff wants to access a site which is blocked and they believe the filtering is being too sensitive, they can apply to the Deputy Head Academic who will investigate the site to ensure that it contains appropriate content before a decision is made whether to allow access to it.

INTERNET ACCESS

Pupils from Reception to Form 8 have access to the Internet in school.

Pupils in EYFS and KS1 are closely supervised when using the Internet and are limited to specified websites. They are taught what to do if they ever see anything which they find scary or upsetting whether this is in school or not.

Pupils from Form 3 upwards use the internet more independently and they are reminded at the start of each year and regularly during the year how to use the internet safely and effectively, and what to do if they see anything inappropriate. With younger pupils, a member of staff will always be on hand to monitor the websites boys are accessing. The Acceptable Use Policy is signed by all staff and parents on joining CCCS. All pupils from Form 3 upwards are asked to sign the Acceptable Use Policy every September and are reminded of its content.

From Form 3 upwards, boys have their own network area where they save their work, but they are taught that the Head of ICT and Computing, the Network Manager and the IT support staff can access these areas if necessary.

Older pupils may have access to the Internet for example during break or lunchtimes or for choristers, during the evenings, but staff are always available should a boy need to refer a concern about internet content to them.

Our Computing curriculum covers what the internet is, how to use its various tools effectively and how to keep safe online. Internet safety is also covered through our PSHE curriculum.

Boys who have a smartphone which they use when travelling to school are required to hand it in at the office during the day. Occasionally staff will allow boys to collect their smartphones for use during a lesson, but their use will be carefully supervised by staff to ensure boys are only using them for the required purpose. Staff are briefed at the start of year staff meeting and regularly during the year at meetings or by email to

remind they about this required monitoring. The same applies to any boys who have other electronic devices capable of access the internet such as Kindles, tablets or a laptop.

MONITORING

Staff have access to the Senso monitoring system. This enables staff to monitor what pupils are doing in real time and to intervene, e.g. freezing the screen of a pupil or taking a screenshot for evidence of inappropriate behaviour. Senso also takes automatic screenshots if it detects unacceptable behaviour. In addition, the Head of ICT receives daily email reports from Schools Broadband on any inappropriate searches.

The Deputy Head Academic provides regular reports on both Filtering and Monitoring to the governors' Compliance Committee.

MICROSOFT COMMUNICATION SYSTEMS

Pupils in Form 3-8 and all staff have a school Microsoft account which gives them access to Outlook (for email), Teams, OneDrive and Office365.

At the start of Form 3 boys are taught how to use their Microsoft Account as well as learning about the appropriate use of the tools within it, including email. They learn that anything which is sent by email or posted on Teams should not be thought of as private and it could be seen by people other than those they intend and that any content which is shared on the internet should be treated as being there permanently.

When in school, pupils are only allowed to use school email. Access to other email systems such as Gmail, or social media, are blocked.

The school Microsoft system (including Teams and email) is monitored by the Deputy Head Academic and the Network Manager. If concerns are raised about any messages being sent or received, the relevant accounts can be accessed and/or the user blocked from accessing their account if necessary. Pupils found to have misused the school Microsoft system are likely to be blocked from using it for a period of time and may also be subject to other sanctions such as lack of network access.

MANAGING WEBSITE CONTENT

The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers is obtained when a pupil joins the school before photographs of pupils are published on the school website or on our social media.

The Headmaster or nominee takes overall editorial responsibility and ensures that content is accurate and appropriate.

The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.