



Cyber Security

Dear parents, prospective parents and agents,

All parents would rightly agree that supporting the physical and emotional needs of the young people in our care is our top priority. Another safeguarding responsibility that we treat just as seriously, however, is our need to **protect the personal and financial interests of our families**.

For that reason, I am writing to you to remind you that cyber crime is a global challenge and that schools such as ours are increasingly seen as targets by would-be attackers.

We are aware of a number of fraudulent emails circulating in the sector that claim to offer significant discounts for the payment of fees in advance. These emails are written with varying degrees of sophistication but some are very realistic and can look like they are coming from a genuine sender. These scams are sometimes opportunistic but are sometimes the result of hackers gaining access to a parent's email, and using information found there to create communications that can look realistic and convincing.

I would like to reiterate that the school will **never under any circumstances** send fees in advance offers or changes of bank details by email.

We insist that fee payments are made by Direct Debit / Flywire wherever possible, which helps to mitigate risk (please note that parents' bank details are never visible to or stored by the School during this process).

Should you receive a suspicious email requesting payments please do not reply to it or call any of the numbers you may find in the email. Always check directly with the school using the usual School contact details on the School's website.

Please note that the school cannot be held responsible for reimbursing any fees in the event of an incident arising from a scam or fraudulent email.

Thank you for your patience and understanding as we stress-test our security. I hope that you are reassured by our proactive and prudent actions.

Kind regards,

Jenny Seed
Head of Marketing and Admissions
Tel. 01303 253 951
admissions@earlscliffe.co.uk



IT INFORMATION

ALL STUDENTS will need a Windows or Mac laptop computer with charger (iPads are not suitable for lessons but can be brought for personal use).

Students should also have a mobile phone with charger to communicate with their House Managers and staff on trips.

Use of mobile phones is restricted during the day but may be used during free time.

WiFi access will be restricted during night times.

Students will be given a school email address for the duration of their stay at Earlscliffe. We recommend you still use your personal email address for private accounts e.g - your evisa, banking, amazon etc

Our school systems are centred around google.

Before arrival please download:

To ALL devices: <https://www.securly.com/ssl> - the webpage will share with you an installation guide suitable to your device.

Alerts - You may get some security alerts whilst installing the certificate. These alerts are designed to protect you against installing certificates from unknown sources. Securly is a known and trusted source so you can ignore these warnings and proceed with the installation.

To mobile phones: Please also download [Whatsapp](#) to allow communications with your house manager and house mates.

For any help with anything IT please contact itsupport@earlscliffe.co.uk.

