The Cherwell School
E-Safety Statement

Whilst exciting and beneficial both in and out of the context of education, much of ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that some have minimum age requirements, usually 13 years.
We take care to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in and beyond the context of the classroom.
This statement is supported by our Acceptable Use Policies for staff, governors, visitors and students in order to protect the interests and safety of the whole school community. It has been approved by the Oxfordshire Safeguarding Children's Board and is linked to the following school policies: Behaviour for Learning Policy, Anti-bullying Policy, Safeguarding Policy, Handheld device policy and Data Protection Policy.
Key staff with oversight of e-Safety are the Deputy Head teacher (student experience and wellbeing), Faculty leader for ICT and Computing and the Network Manager.

Content

The Cherwell School operates a web filtering system to reduce access to illegal, inappropriate or harmful material. This filtering is applied to all access to the Internet from school PCs, laptops, Chromebooks and any other device using the school wifi, including personal devices. The level of filtering is tailored to each key stage, for example KS4 & 5 have open access to Youtube, whereas for KS3 this is only available to channels deemed educational by Youtube. Additionally, teachers are able to allow access to specific sites to specific students for a limited amount of time when required. They are given guidance on what they should consider when allowing access to 'blocked' sites. All Internet activity is logged and monitored.

Contact and Conduct

Issues relating to contact and conduct online are addressed through a range of activities and lessons, such as ICT lessons, RS/PHSCE lessons, tutor time and assemblies. All staff are given updated training at least once a year as part of safeguarding. Topics covered include:

- Digital footprints
- Social media
- Data Security
- Cyberbullying
- Grooming
- Youth produced sexual imagery and Sexting
- Identity Theft

Any issues can be reported by students either internally via an online form (which can be anonymous) or via email (esafety@cherwell.oxon.sch.uk) or externally to CEOP via links on our Intranet page.

Responding and Managing Sexting Incidents

The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

If we become aware of intimate images being sent we will follow the SWGfl and UK Safer Internet Centre guidance which is supported by DfE.

STAFF WILL NOT VIEW OR ANY SEXTING IMAGES, NEITHER WILL THEY FORWARD SUCH IMAGES TO ANY OTHER PARTY.

Step 1:
If a device is involved – staff will confiscate it and set it to flight mode or, if this is not possible, switch it off.

Step 2:
The incident will be reported to the designated safeguarding lead via normal child protection procedures.

The Designated Safeguarding Lead will record all incidents of sexting, including the actions taken as well as not taken and give reasons. In applying judgement to each incident, consideration will be given to the following:

- Is there a significant age difference between the sender/receiver involved?
- Is there any external coercion involved or encouragement beyond the sender/receiver?
- Do you recognise the child as more vulnerable than usual i.e. at risk?
- Is the image of a severe or extreme nature?
- Is the situation isolated or has the image been more widely distributed?
- Have these children been involved in a sexting incident before?
- Are there other circumstances relating to either sender or recipient that may add cause for concern i.e. difficult home circumstances?

If none of these circumstances are present, then the situation will be managed within school and without automatically escalating to external services. Details of the incident, action and resolution will be recorded in safeguarding files. Information may be shared with other schools where appropriate to limit the distribution of the image and safeguard students on their roll

If any of these circumstances **are** present, then the incident will be referred to relevant external agencies including MASH and the Police

GDPR

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Our Acceptable Use Policy is for all staff, governors, visitors and students and is inclusive of both fixed and mobile internet technologies provided by the school (such as PCs Laptops, mobile devices, webcams, whiteboards, digital video equipment etc) as well as technologies owned by pupils and staff but brought onto school premises (such as laptops and mobile phones)

Information for Parents

Parents are provided with education and guidance through regular e-Safety presentations, which are organised with the PTA, and via information on the school website.

Sanctions

Where necessary, inappropriate use is addressed through one of the following policies:

- ICT Acceptable Use Policy
- Behaviour for Learning Policy
- Anti-bullying Policy
- Safeguarding Policy
- Handheld device policy
- Data Protection Policy
- Staff Code of Conduct Policy
- Home School Agreements

November 2019