Warlingham School
& Sixth Form College

Wide Horizons
High Aspirations

ONLINE SAFETY POLICY

Introduction

This policy is focussed on the knowledge and behaviours that will help students and staff to safely benefit from the online world, regardless of the device, platform or app that is used. Specific guidance is available separately (for example an Acceptable Use Agreement) and this will be regularly reviewed in the light of technological changes and experience. This policy builds on the requirements of 'Keeping Children Safe in Education' and hyperlinks to the main sources of guidance are at the end of this policy.

Learning for safety

The school will ensure that students and staff understand how to use online school systems safely and that this knowledge is regularly updated. For staff this will be through regular staff training and for students it will be through the taught curriculum (Relationships and Sex Education, Health Education, Computing and other subjects) together with the broader curriculum (Safeguarding, guidance and opportunities such as assemblies). Where appropriate, the latter will be supported by activities for students' families.

Knowledge and Behaviours

There are five key outcomes that the online curriculum will help students achieve. These combine developing knowledge with an understanding of the student's behaviour and that of others, both on and offline.

- How to **evaluate what they see online** – The ability to make judgements about what they see and to ask themselves whether it is: Fact or opinion? Too good to be true? Fake or genuine? Fair? Acceptable?

- How to recognise when approaches are being used to **convince them to think or respond in a particular way**. To continue gaming, to buy something or to spread false information.

- To **recognise and practice acceptable online behaviour** - A high standard of behaviour and honesty is expected both online and offline. This includes understanding the effects of online anonymity, how peer pressure intensifies emotions and techniques to deal with conflict and negative language. To behave appropriately during remote learning, with regard to working and communicating with the teacher and other students.

- How to **identify online risks** – Having the knowledge of a range of online risks to recognise these behaviours and then decide on the best course of action. This requires the development of judgement in respect of sharing personal information, when to participate in an activity and that a digital footprint can be viewed many years in the future.

- **How and when to seek support** – Who to turn to if they are concerned or upset by something they have seen online. To know the adults they can trust, as well as knowing how to access support from school staff and organisations such as the police, Childline and CEOP. They should also know that platforms and apps will have ways in which inappropriate contact or content can be reported.

Risks

The students' learning about online safety will develop knowledge and skills to ensure they enjoy safe and positive experiences online. The rapidly changing nature of online technology means that risks will change and the following highlights the main areas of risk considered by the whole curriculum.

Using the internet and the information it contains:

- Age restrictions to protect young people
- How content can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Online fraud
- Password phishing
- Gathering personal data
- Persuasive design
- Privacy settings
- Targeting of online content

Staying safe online:

- Online abuse
- Online challenges
- Content that incites – hatred or violence
- Fake profiles
- Grooming
- Live streaming a video, usually of yourself
- Pornography
- Communicating with people you have not met

Wellbeing:

- Impact on confidence, particularly body image
- Impact on physical and mental health
- People behaving differently online and offline
- Long-term reputational damage
- Highlighting of self-harm and eating disorders

Within any group of students or staff, some will have personal experience of the impact of these risks. Others may be particularly susceptible to online harm or have less support from family or friends. The school will be proactive in ensuring all who may be potentially affected in this way, receive the information and support they need. This will be achieved through good communication between staff and the maintenance of a highly positive Safeguarding environment in which all feel supported in raising issues.

Network Security - Filters and Monitoring

As part of the school's work to reduce online risks, it has in place a range of filters and monitoring systems. The choice of appropriate tools has been informed by a risk assessment that reflects the age and experience of our students. While online safety is the main priority, a balance will be maintained between safety, use of resources and the dangers of 'over blocking'. Mobile technology presents challenges for network security both at school and at home. The knowledge and skills gained through the curriculum will help students keep themselves safe online when using mobile technology outside of school. However, families must ensure that comparable filtering systems are in place to support students at home.

Staff Training

All new staff members will receive training as part of their induction on online safety (including grooming, cyber-bullying and the risks of online radicalisation). All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates through emails, bulletins and staff meetings. The Designated Safeguarding Lead and deputies will undertake child protection and safeguarding training, including online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Users will also be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss.

Monitoring and Review

Records of any online safety incidents will be kept by the Safeguarding or IT teams as appropriate. These will be reviewed by the responsible member of the Senior Leadership Team as necessary and at least termly. They will also be responsible for providing Governors with summary information to enable them to make a judgement about the fitness for purpose of this policy at the time of review.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign and agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Inappropriate use of mobile phones on the school premises

If a student has been seen filming or taking photos on the school premises the student will be requested to delete the footage and the phone confiscated for parental collection This will result in a sanction from the school. If the footage is uploaded onto social media the school will take the decision to suspend the student and depending on the severity of the incident report this to the police. All incidents of this type will be recorded on the students record.

Please also refer to:

DFE Teaching online safety in school June 2019

Keeping Children Safe in Education (KCSIE)

DFE Relationships and Sex Education, and Health Education 2019

DfE Searching, screening and confiscation

DfE Protecting children from radicalisation

DfE Preventing and tackling bullying and cyber-bullying

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy should be read in conjunction with the following policies:

- Anti-bullying Policy
- Behaviour for Learning Policy
- Child Protection Policy
- Safeguarding Policy
- Code of Conduct and Staff Behaviour Policy
- ICT Use and Online Safety Policy
- Mobile Phone Policy

Approved by Local Governing Body	Summer 2023
Due for review	Summer 2024
SLT Member	Ms K Haynes