Online Safety Policy for Day School and Sixth Form

Introduction

The welfare of all pupils is our primary responsibility. Every adult who works at the School is aware that they have a responsibility for keeping all pupils safe at all times and this includes online safety.

Technological developments such as the internet and other forms of electronic communication have great educational and social benefits, but they can also be used to harm others. The School understands the responsibility to educate pupils about online safety issues, to teach them appropriate behaviours when using the internet and related technologies in and beyond the classroom. It is also committed to establishing a clear set of expectations around the online behaviour of both pupils and staff.

This policy applies to all members of the School community (including staff, pupils, parents, visitors and trustees) who have access to and are users of the School's IT systems, both in and out of the School. This policy covers both fixed and mobile devices provided by the School, as well as devices owned by pupils or staff and brought onto School premises. The policy, supported by the other relevant policies listed below, seeks to protect the safety of pupils and staff.

Other Relevant Policies

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

- IT Acceptable Use Policy
- Safeguarding Policy
- Anti-Bullying Policy
- Data Protection Policy
- Behaviour, Rewards and Sanctions Policy

Education

ArtsEd reinforces internet safety messages to all pupils at regular intervals and at an age-appropriate level through the curriculum.

Issues covered include the following:

- Safe and appropriate use of social networking sites (specifically age-appropriate)
- The issues surrounding excessive use of games consoles, internet gaming sites, mobile phones (especially texting) and social networking or messaging facilities
- The sending of inappropriate photos via mobile phone or the internet
- The dangers of illegal and harmful substances sold online

- The effect on pupils' wellbeing and self-image of social media and other messages that they may get from online activity
- The effect of internet pornography on pupils' self-image and their relationships with others
- The dangers of communicating with others online

Members of staff are informed of the IT Acceptable Use Policy for Staff which explains their responsibility for safe and appropriate use of the School's IT systems.

Online Safety is a focus of all areas of the curriculum and staff reinforce Online Safety messages across the curriculum. The Online Safety curriculum is broad, relevant and provides progression, and will be provided in the following ways:

- An Online Safety curriculum is provided as part of the Digital Learning Certificate
- Key Online Safety messages are reinforced as part of a planned programme of whole school PSHEE
- Pupils are taught to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- When they join the School, pupils are asked to read and agree to an IT Acceptable Use Policy for Students document which outlines protocols for the use of School equipment and their own devices.
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

Parents

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviour. This advice is drawn from recommendations made by CEOP:

- Make yourself aware of the amount of time your child is using the internet, chat facilities, games consoles and their mobile phones and whether this is excessive.
- Consider carefully the location of the computer or laptop and whether your child would be better using it in a family area of the home.
- Search on Google and other search engines for your child's name and any online usernames they use. This is a valuable exercise for you and them to see exactly how much other people can see about them with very little difficulty
- Consider installing internet monitoring software on home computers
- Talk to your child; both about the dangers or the internet, but also about their general usage – be interested in what they are doing and keep a dialogue open so they feel able to talk to you if they do experience problems
- Ask your child to (or help them) set up appropriate privacy settings on Facebook and other social media platforms.

Staff

Staff receive training on INSET days as well as throughout the year on IT and Online Safety issues. The Staff Code of Conduct and Staff Handbook also contain sections with advice on staff communication with pupils, staff internet use and staff use of social networks.

Use of devices, the internet, email and other forms of digital technology

The School sets out clear rules and guidance for pupils regarding the use of devices, digital technology and the School's network. Expectations are explained clearly in the IT Acceptable Use Policy that all pupils are required to agree to. The School's rules and disciplinary procedures associated with the misuse of devices, digital technology and the network are explained in the Behaviour Rewards and Sanctions Policy

Confiscation and searching of pupil devices: an electronic device such as a mobile phone or a tablet computer may be confiscated in appropriate circumstances in accordance with the Behaviour Rewards and Sanctions Policy. If there is good reason to suspect that the device has been, or could be used to cause harm, to disrupt teaching or break school rules, any data or files on the device may be searched and, where appropriate, data or files may be erased before the device is returned to its owner. The expectations of staff for using the internet, email and other forms of digital technology are set out in the Staff Code of Conduct and Staff Handbook.

Filtering and Monitoring

As part of its Safeguarding duty, the School has put in place filtering and monitoring to try to ensure children are safe when accessing the internet in school. The School's network uses filtering software for all website activity, and appropriate age restrictions applied. The Safeguarding team receives reports on staff and pupil use of the School's network and online activity.

Behaviour and Anti-Bullying (See school Anti-bullying Policy)

Cyber-bullying by pupils will be treated as seriously as any other type of bullying, and will be managed through our anti-bullying procedures, and they can be escalated to safeguarding concerns.

The appropriate School disciplinary procedures are followed in relation to any incident of misuse of IT equipment or websites or of cyber-bullying. The School reserves the right to take action - even when the offence is committed outside of School - if it harms members of our community or brings the School into disrepute.

Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, against a victim who cannot easily defend him/herself. It is sometimes also known as 'online abuse' as the term cyber-bullying can become trivialised through overuse. Mobile, internet and wireless technologies have increased the pace of communication and brought benefits to users worldwide. Unfortunately, however, their popularity provides the opportunity for misuse through cyber-bullying.

Cyber-bullying includes: Text message bullying; picture/video bullying via mobile phone cameras; phone call bullying via mobile phone; email bullying; chat room or social network bullying; bullying through instant messaging; bullying via websites; bullying via gaming platforms.

Ways pupils can keep themselves and others safe include:

- Not posting personal items (including photographs) or information– keep information general.
- Thinking carefully about posting pictures online – once it is there, anyone can see it or use it.
- Not sharing passwords –personal information should be kept private!
- Never meeting up with someone they have 'met' online without a responsible adult being present

- Thinking carefully before writing anything online – people can misinterpret words.
- Respecting other people's views – there is no need to be rude or abusive if opinions differ.

What can a pupil do if they a victim of cyber bullying:

- Tell someone they trust.
- Report any cyber-bullying, even if it is not happening to them.
- Never respond/retaliate as it could make matters worse.
- Block the cyberbullies.
- Save and print any bullying messages, posts, pictures or videos that are received or seen online so that they can be passed on to the School or other authorities, should this be required. Make a note of the dates and times they are received.

Sexting and revenge porn are taken particularly seriously and pupils are educated about the dangers and possible consequences of these acts through PSHE lessons and the wider curriculum.

Cyber bullying is explicitly referred to in the School's Anti-Bullying Policy and the School's expectations of pupils in this area are clearly set out in the policy.

Sexting

Sexting has been defined as 'Youth produced sexual imagery': it involves children sharing images that they, or another child, have created of themselves. A child in this context means anyone under the age of 18. 'Imagery' covers both still photos and moving videos which are increasingly common. Pupils and parents are educated through the PSHEE and wider school curriculum on the particular dangers of sexting and revenge porn. As well as discussing the moral and social issues surrounding these, a particular focus on the legal consequences of engaging in these activities is given. This includes reference to recent advice on schools and police on how to deal with sexting.

When the School becomes aware of a sexting incident, it will follow the procedures and guidance as set out in DfE *Sharing of Nudes and Semi-Nudes: advice for education settings working with children and young people (2020)* If a member of staff becomes aware of a sexting incident, then they must report it to the Designated Safeguarding Lead. The staff member will **never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.

The Designated Safeguarding Lead will usually interview the children involved (if appropriate). Parents will usually be informed at an early stage and involved in the process (unless there is good reason to believe that involving parents would put the child at risk of harm). At any point in the process if there is a concern a child has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately. The School's sanction system will also be used depending on circumstances (refer to the school's Safeguarding Policy and Behaviour Rewards and Sanctions Policy which refers to sexual misconduct and the possession and supply of indecent imagery).

Online Safety: Safeguarding and "Prevent"

Some adults and young people may use technologies to harm children and the School is aware of the Safeguarding concerns linked to Online Safety. KCSiE 2021 outlines three areas of risk:

(i) online content (being exposed to harmful material);

(ii) contact (being subjected to harmful interaction with others online); and

(iii) conduct (personal online behaviour that increase the likelihood of, or causes, harm).

When necessary, the Trust will inform the police or Hounslow Safeguarding Children Partnership if they have concerns about the online activities of pupils at the School.

The Counter-Terrorism and Security Act 2015 places a duty on specified authorities, including Schools, to have due regard to the need to prevent people from being drawn into terrorism (“the Prevent duty”). As part of the School’s “Prevent duty” the issue of extremist or terrorist material on the internet is covered in PSHE lessons. The School’s filtering and monitoring systems ensures children are safe from accessing terrorist or extremist material when using the internet in School. The School’s Safeguarding Policy explains in more detail how ArtsEd address these issues.

Review

This policy is reviewed annually by the Deputy Headteacher and the Head of IT.

Document Title	Online Safety Policy
Maintained By	Nick Granville
Owned By	Nick Granville
Approving Committee / Ratifying Body	Board of Trustees
Last Reviewed on	September 2021
Review on	September 2022
Current Version	Version 1
Location of master document	ONLINE SAFETY POLICY.docx (sharepoint.com)
Web location	ONLINE SAFETY POLICY.docx (sharepoint.com)