Guildford County School

E-Safety Policy

Policy Review
This policy was adopted March 2021
It will be reviewed in March 2022
by the Impact Committee - Guildford County School Governing Body

Guildford County School
E-Safety Policy and Procedures

Our Policy

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4/5G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

E-safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

Our E-Safety Policy therefore aims to:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children and young people to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The risks

The risks to which children and young people are exposed online are still not as well understood as they need to be, and parents' and staff awareness and knowledge often lag behind those of the students in their care. 83% of 12-15 year olds now own smartphones (OFCOM, 2017) most including cameras and with broadband internet access. Half of this age group have access to the internet at home "mostly alone", without an adult present (OFSED, 2013). Being asked to share intimate photos of their bodies is considered "mundane" by most Year 9 girls (NSPCC, 2012). A quarter of 12-15s say they use social networking sites to communicate with people not directly known to them (OFCOM, 2012). Almost a third of KS3 and KS4 students report being harassed, targeted or bullied online, with girls, SEND students and those from poorer socio-demographic backgrounds most at risk (OFSTED, 2013). The widespread availability of and desensitisation to pornography among boys in particular is now an accepted phenomenon. In addition, young people are exposed to risks unrelated to age, such as identify theft or fraud.

Our approach acknowledges the existence of the following risks, grouped into three categories: Content, Conduct, and Contact. Note this (non-exhaustive) list is for summary purposes only, rather than a full description of each.

Content risks

- Exposure to offensive or age-inappropriate material, including pornography and violence
- Exposure to sites promoting self-harm, including substance abuse and eating disorders
- Breach of copyright, intentional or unintentional
- Accepting inaccurate, unreliable or intentionally misleading information as factually correct
- Plagiarism of another's work
- Commercial promotion to under 16s, in defiance of the UK CAP code
- Unsolicited advertising or promotions ("spam")
- Unsolicited messages containing links to offensive material

Conduct risks

Definition: personally identifiable information (PII) is any information online that could be used, possibly in conjunction with other information, to identify and make unsolicited contact with someone, or to pretend to be someone. Examples include names (including names contained within usernames), postal addresses or postcodes, email addresses, dates of birth, telephone numbers, photos or videos, friends', siblings' or teachers' names, car number plates, membership of clubs or societies etc.

- Theft or misuse of PII by third parties, including identity theft
- Phishing i.e. fraudulent soliciting of PII or security access credentials
- Theft of devices containing PII, e.g. phones, tablets
- Infection of malware and viruses
- Exposure of another person's PII e.g. a friend or sibling
- Weak or compromised password protection
- Weak privacy settings
- Libel, slander and contempt of court
- Damage to personal reputation

Contact risks

- Friending of or by strangers
- Requests for self-generated indecent images ("sexting") either by fellow students or unknown online users, possibly posing as "friends" and using blackmail techniques
- Harassment and bullying using online channels
- Grooming
- Inappropriate contact by or with children in care or other vulnerable young people
- Addictive tendencies e.g. to online game sites
- Commercial scams and frauds
- Upskirting
- Sexting

Radicalisation

Radicalisation is covered in detail under the **Prevent Strategy** section of the Child Protection Safeguarding Policy. As part of our ongoing work to prevent radicalisation GCS considers and discusses threats which could be posed through the internet and social media and reviews e-safety education in the light of these widening and extreme risks.

Prevent Co-ordinators are in place on behalf of Surrey County Council, Prevent Co-ordinators at the school constantly review e-safety, monitor searches and terms and constantly update filters on the school systems to protect students. Our nominated Prevent co-ordinator can be contacted with any concerns at: jcole@guildfordcounty.co.uk

Roles and Responsibilities

The Governing Body

The governing body will:

- ensure that a senior member of staff acts as co-ordinator for promoting e-safety.
- nominate a link governor who will liaise with the co-ordinator over her/his reports to the governing body.
- monitor and evaluate the effective implementation of this policy.

The Headteacher

The headteacher will:

- ensure that online safety, including awareness-raising of the above identified risks, is part of the ICT curriculum (or in other appropriate subject areas of the curriculum) in each year group.
- appoint a co-ordinator who will receive specialist training.
- ensure that all school staff are aware of the policy and are able to implement it.
- ensure that the school complies with the requirements of the Data Protection Act 1998, and that access to students' personal data is appropriately controlled.
- ensure that all parents are aware of this policy.
- monitor and evaluate the effectiveness of this policy.

The Co-ordinator

The coordinator will:

- undertake regular personal e-safety training
- ensure that effective training, guidance and support are provided for all school staff to help them be alert to and discourage risk-taking behaviour
- ensure that all students are aware of who they can talk to if they are concerned by anything that they see online that makes them feel worried or uncomfortable
- respond to reported concerns and incidents seriously and sensitively, providing support to students as appropriate
- provide opportunities for parents and students to ask questions and seek guidance about online risks
- keep the school community aware of specific or new risks that come to light, and amend the above list accordingly
- in conjunction with the leadership team and the key stage team respond to and deal with all reported incidents of bullying online or via digital communication media
- keep up to date with new developments and resources to address bullying
- support students who have been bullied and those who use bullying behaviour
- keep records of all reported e-safety incidents
- report annually to the governing body on the extent of online bullying and the effectiveness of this policy
- Ensure safeguarding is considered in the school's approach to remote learning

Staff

Staff will:

- undertake appropriate training to ensure they are familiar with the above risks
- be aware of and alert to signs of misuse of the internet and social communication media
- report all incidents of bullying online or using social communication media or other e-safety incidents

Parents and Carers

Parents and carers are expected to:

- familiarise themselves with this policy and the risks their children may be exposed to online, including the relevant sections of the CEOP site www.staysafeonline.com

- understand how to operate “parental controls” on the internet-enabled devices to which their children have access
- be familiar with age restriction advice (eg PEGI rating for games)
- take an interest in their children’s activities online, maintaining an open dialogue about both positive and negative aspects
- be familiar with the options their children have to report concerns
- inform the school if they do not wish their child’s image to appear in photographs or videos published by the school
- ask for further information or guidance should they require it

Students

Students are expected to:

- look after themselves and their friends online, and report anything they are concerned by or anything that they see online that makes them feel worried or uncomfortable
- help the school keep this policy relevant and up to date by feeding back comments and suggestions, including through the student council
- Adhere to the school’s Acceptable Use Policy

Procedures

The curriculum

We will:

- ensure that the curriculum addresses the risks of inappropriate online behaviour
- ensure that students are aware of what internet use is acceptable and what is not and given clear objectives for internet use
- ensure that students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- ensure that students are shown how to publish and present information appropriately to a wider audience
- ensure that students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- liaise with the PHSE co-ordinator to ensure that the sex and health education curriculum addresses the likelihood that many students will have been exposed to pornography and self-harm sites

Managing access

We will:

- seek to ensure that the use of internet derived materials by staff and by students complies with copyright law
- review school ICT systems security and security strategies regularly
- implement and update virus protection on the school networks and devices
- filter sites for different age groups as appropriate, while recognising that most networks which students use have limited or no filtering, and seeking to avoid restrictions wherever possible which might limit students' learning experience
- maintain an Acceptable Use Policy for the school's own network and operate a "block list" of known inappropriate websites
- be aware of the benefits of new and emerging technologies and carry out risk assessments before permitting their use in school
- permit and support the use of mobile phones and other handheld electronic devices during lessons and other school activities where they enhance learning and the curriculum
- direct staff to use school email addresses for all communication between the school and students or parents/carers
- monitor staff and student use of school electronic communication and respond appropriately to unacceptable use
- consider how email from students to external bodies is presented and controlled
- encourage students to treat incoming email as suspicious and not to open attachments unless the author is known

Published content

We will:

- provide contact details on the school website: the school address, email address and telephone number
- make available staff school email addresses, essential identification and contact information, but not publish staff or students' personal information
- seek to ensure that published content is accurate and appropriate
- seek to ensure that published photographs and recordings of students take account of the need to protect vulnerable students
- obtain written permission from parents or carers before photographs of students are published on the school website
- inform parents of the school policy on image taking and publishing

Social networking

We will:

- control access to social networking sites, and educate students in their safe use e.g. use of passwords
- advise students never to give out personal details of any kind which may identify them or their location
- advise students and parents that the use of social network spaces outside school brings a range of dangers
- encourage students not to reveal personal details of themselves or others in email communication, when using social networking sites, or arrange to meet anyone without specific permission

Reporting concerns or incidents

We will:

- refer complaints and concerns about inappropriate use of email and electronic communications media to any senior member of staff
- refer complaints and concerns about inappropriate staff use to either the headteacher or co-ordinator
- manage complaints or concerns in relation to child protection in accordance with our safeguarding policy and procedures
- inform students and parents/carers of the consequences of transgression in using email and electronic communications media
- supervise and set clear reporting procedures for staff who manage ICT systems and monitor email and electronic communications media

Students should report any incidents they encounter or concerns they may have

- to their parents or carers
- to any teacher or tutor, or the school office
- to the e-safety co-ordinator or the headteacher
- anonymously to the school through me@guildfordcounty.co.uk
- to a third party service such as CEOP (https://www.ceop.police.uk/safety-centre/) or Childline (http://www.childline.org.uk/)

Parents and carers should report any online safety issues they become aware of to the e-safety co-ordinator Jo Cole jcole@guildfordcounty.co.uk or to the headteacher.

Remote Learning

- Remote learning takes place using MS Teams as a platform.
- Students are to keep cameras off while they are learning at home, taking part in live lessons.
- Where one-to-one sessions are organised, either another member of staff should be on the call or the meeting should be recorded.
- All must maintain the standard of behaviour and language expected in school.
- The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed and can establish secure connections to allow participation in live lessons.

Review

This policy will be reviewed by the Impact Committee annually.

Related policies include the Anti-Bullying and Safeguarding Policies which are available on the school website.

Useful Resources for Teachers and Parents

Resource	Website

Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school