

Stanstead Flying High Academy



E-Safety and Online Policy 2023-2024

To be reviewed September 2024



Roles and Responsibilities

It is the responsibility of all adults and pupils linked to Stanstead Flying High Academy to ensure that this policy is implemented fully. All staff and visitors must sign an 'Acceptable Use Policy/ICT Code of Conduct' and adhere to it at all times.

The school computing lead is Chloe Jenkins and the member of the Senior Leadership Team and DLS responsible for E Safety is Tanya Smith.

Online Safety

As a school, we are aware that online safety has a considerable breadth of issues, which fall under the following areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users, for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. We are aware that if we feel that our pupils, students or staff are at risk, we must report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Teaching and Learning

Why internet and digital communications are important

- The purpose of technology in school is to raise educational standards, to promote achievement, to support professional work of staff and to enhance the school's management functions.
- Stanstead Flying High Academy has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

- They will be taught what internet use is acceptable, and what is not, and be given clear objectives for use. These are also important transferrable skills for their life out of school, including with the use of mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.
- We include issues such as Cyberbullying and e-safety in our curriculum to encourage self-efficacy and resilience. We ensure we support all children where necessary.

Managing Internet Access

The school's ICT system security is reviewed regularly and our virus protection is regularly updated.

Filtering and Monitoring

To safeguard and promote the welfare of children at our school and provide them with a safe environment in which to learn, we limit children's exposure through appropriate filtering and monitoring on school devices and school networks. Regular reviews take place to identify their effectiveness. The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Consideration is taken in to account to the number of and age range of children in the school and those who are potentially at greater risk of harm, with regards how often they access the IT system.

The school and Academy Trust identify and assign roles and responsibilities to manage filtering and monitoring systems.

- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet safeguarding needs

The school's Academy Trust has enabled Atom IT services to carry out and provide support with reviewing filtering and monitoring.

The LGFL Online Safety Audit and Risk Assessment is carried out annually by the online safety lead- Tanya Smith and is then shared with the DSL team.

Parental communications to reinforce the importance of children being safe online is provided to understand of what systems the school use to filter and monitor online use. The importance for parents and carers to be aware of what their children are being asked to do online, is taken in to account, including the sites they will be asked to access and who their child will be interacting with online.

The school has additional policies that support/ identify filtering and monitoring, including- Online safety and is informed in part, by the risk assessment required by the Prevent Duty.

Email

Staff may only use approved e-mail accounts on the school system.

- All in-coming e-mails should be treated as suspicious and attachments should not be opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published Content and the School Website

- The contact details on the school's website are the school address and phone number; no staff or pupil's personal details will be published.
- The Headteacher has overall editorial responsibility of the website to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include identifiable images of children should only be added to the school's website, X (formally known as Twitter), Facebook, Class Dojo accounts with consent from the parent/carer.
- Pupil's full names will be avoided on the website, especially with associated photographs.
- Parents are informed about our school policy on image taking and publishing.

Social Networking

- The school does not allow use of any social network sites for children.
- The school uses private and secure X (formally known as Twitter), and Facebook accounts.

Mobile Phones

- Any mobile phones brought into school, are required to be handed to the school office and returned at the end of the school day.
- The school recognises youth produced sexual imagery, sharing of nude and semi-nude images (previously known as "sexting") as a safeguarding issue; all concerns should be reported to and dealt with by the Designated Safeguarding Lead (DSL).
- The school recognises the need for children to be kept safe from terrorist and extremist material; therefore, it will be covered by the e-safety curriculum.

Video Conferencing

- Video conferencing is always supervised.
- Any video conferencing will use the educational broadband network to ensure quality of service and security.

Managing Emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or school time as

part of an educational activity.

- Care will be taken with the use of hand-held technologies in school which may not have the level of filtering required.
- Staff will only use school phones for contact with pupils and their families.
- In the event of staff working from home, 141 must be used before any phone call are made.

Network management (user access, backup)

- The school uses individual, audited log-ins for all staff users.
- Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).
- Pupils and staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Policy Decisions

Authorising internet access

- All staff, governors and visitors must read and sign the 'Acceptable Use/ICT Code of Conduct' before using any school ICT resource.
- Parents will be asked to sign and return a consent form.

Assessing Risks

- The school will take reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on a school ICT resource.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

Arrangements for reporting e-safety incidents

Inside School

- Any incident must be reported to a child's class teacher as soon as possible.
- If available, any evidence must be kept.
- Statements must be taken from all parties involved.
- A member of the Leadership Team must be informed and decide on the best course of action – this may include school-based sanctions, meetings with parents and, in the most severe incidents, the police may be involved.
- All incidents must be recorded and logged.

Outside School

- As soon as a member of staff is made aware of any e-safety incident, they must follow the guidance above.

- Parents should always be informed when e-safety incidents occur outside of school.

Children are regularly reminded of how to keep safe online and if any incidents were to occur, what they must do. They are also made aware of CEOP www.ceop.police.uk and Childline www.childline.org.uk 0800 1111.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the headteacher.
- Complaints of misuse by staff will also be dealt with by the headteacher.
- Any complaints of a child protection nature will be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with our Behaviour Policy.

Community use of the internet

All use of the school internet connection by community or other organisations shall be in accordance with our e-safety policy.

Communicating Our Policy

Pupils

- Appropriate sections of this policy will be shared with pupils.
- E-safety rules will be visible around school and pupils will be involved with the development of these.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be given a copy of the e-safety policy and will sign the acceptable use policy.
- Staff will be made aware that the system is monitored and that professional standards are expected.
- In line with KICSIE 2023, new staff have online checks carried out as part of our recruitment process.

Parents

- Parents will be notified of the policy in newsletters and on the website.
- All parents/carers will be asked to sign the pupil/parent agreement when they register their children.
- Supportive information will be made available to parents to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

This policy links to the following policies:

- Safeguarding Policy, Anti-bullying Policy, Behaviour Policy, Staff Code of Conduct.

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Keeping Children Safe in Education September 2023

Online Safety within 'Keeping Children Safe in Education' 2023 states that: It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

- Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures.
- This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
- Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks
- Considering the 4Cs (above) will provide the basis of an effective online policy.
- The school should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.
- Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

Filtering and monitoring

- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system.
- As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness.
- They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.