CIC
SPORTING STARS
achieving a brighter future

10-JAN-2023

SAFEGUARDING AND MONITORING OF IT SYSTEMS

Trained authorised staff & employees of our Managed IT Service Provider (MSP) may inspect IT equipment or accounts owned, leased or managed by the School.

The School's web filtering and device monitoring services are provided by Cisco, Datto and Watchguard and managed by our IT services provider Hixon Group Limited (MSP).

The School requires all users of the wireless and local network to login using their school supplied credentials. We constantly monitor online activity and can identify individuals as part of this process.

It is the responsibility of the School, to ensure that anti-virus protection is installed and kept up to date on all school machines, compliance is monitored 24/7 by our IT Services provider.

Pupils & staff must never interfere with any monitoring software installed on the School's IT equipment. If there are any issues related to viruses or anti-virus software, the IT Single Point of Contact (SPOC) will inform our IT services provider immediately to resolve.

Please Note: It is not the School's responsibility to install or maintain virus protection on any personally owned devices.

CONTENT FILTERING

The School has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education (September 2022) and the Prevent Duty. The School and our partners are constantly reviewing industry trends to improve filtering and monitoring of internet use in accordance with Keeping Children Safe in Education and any other Department for Education and online safety statutory guidance including SWGFL & the UK Home Office.
We Recognise that no filter can guarantee to be 100% effective, however we are satisfied that the filtering system manages and blocks the following content categories (and web search) content:

ILLEGAL CHILD SEXUAL ABUSE MATERIAL (CSAM)	Content that shows indecent images or sexual acts involving under 18 year olds	**UNLAWFUL TERROIST CONTENT**	Promotes terrorism and terrorist ideologies, violence, or intolerance
DISCRIMINATION	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010	**DRUGS / SUBSTANCE ABUSE**	Displays or promotes the illegal use of drugs or substances

EXTREMISM Promotes terrorism and terrorist ideologies, violence, or intolerance

PORNOGRAPHY Displays sexual acts or explicit images

SELF HARM Promotes or displays deliberate self-harm (including suicide and eating disorders)

MALWARE / HACKING Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

PIRACY AND COPYRIGHT THEFT Includes illegal provision of copyrighted material

VIOLENCE Displays or promotes the use of physical force intended to hurt or kill

Please Note: This list should not be considered an exhaustive list and other content may be restricted based on feedback or recognised online safety risks.

To ensure the safety of all users we regularly test the effectiveness of the filtering system using a range of online testing tools recommended by SWGFL Test Filtering & Open DNS.

REMOVABLE MEDIA

Removable media (personal or for school use) should not be used on school devices.

UNAUTHORISED SOFTWARE INSTALLATION

Pupils are not permitted to download programs on school-based technologies without seeking prior permission from the senior management team.

PERSONAL DEVICES

We recognise that pupils and staff can access the internet over personally owned mobile phone 3G/4G/5G connections. Parents & Carers are strongly advised to make use of the filtering and monitoring facilities provided by their mobile phone operator on these connections.

FOR FURTHER INFORMATION

Please visit: www.sportingstarsacademy.com or;
Email us at: admin@sportingstarsacademy.com