Wilson Stuart School

A Special Academy

Wilson Stuart Online Safety Policy

Keeping Our Pupils Safe Is Our Main Priority

Date adopted: December 2023

Contents

Staffing Key		
Initials	**Name**	**Position**
SH	**Simon Harris**	**Executive Head Teacher**
SP	**Sian Parker**	**Head of Primary**
LD	**Liz Dean**	**Head of Secondary (DSL)**
LM	**Liz Morgan**	**Associate Head of Primary**
TE	**Tom Elmes**	**Associate Head of Secondary**
RP	**Ryan Perrens**	**Computing Coordinator/CEOP Ambassador**
LN	**Leigh Noble**	**Personal Development Lead**
RT	**Raymond Tong**	**Lead IT Technician**
JB	**Jo Bowen**	**Head of 6th Form**

Version Control

Version 2.1 – November 2023

Rationale

Online learning, creative and collaborative resources enrich students' experiences of learning in dramatic ways. In addition, the modern young person is a "digital native" in that they use a myriad of online and mobile tools with great confidence, enthusiasm, and flair to communicate record, document their lives and entertain themselves.

With this familiarity comes risk. There are horrific crimes being committed online, including cyberbullying, child pornography, child abuse, child trafficking and fraud. Many young people are not experienced enough to fully understand the risks of using online tools and the consequences their actions may bring. This policy provides a framework for the school to take measures to protect our students and other stakeholders from these risks and to support them in becoming confident, online safe citizens.

The Online Safety Policy is an integral part of the school's day to day practice and relates to other policies including those for ICT, bullying and for child protection. Roles

Executive Head Teacher ("H/T") (Simon Harris)

- Takes ultimate responsibility for Online Safety policy and practice within school.
- Communicates with Governing Body on Online Safety matters.
- Supports Online Safety Coordinator in the implementation of the policy.

Governing Body (Ruth Hopkins)

- Supports H/T and other designated staff with regard to Online Safety related matters.
- Ensures funding is available to implement and maintain Online Safety.
- Reviews reports on Online Safety.

Online Safety Coordinator (Ryan Perrens) Personal Development Lead (Leigh Noble) / Lead IT Technician (Raymond Tong)

- Reports to / updates the Executive Head Teacher.
- Communicates with other key members on Online Safety related matters.
- Responsible for development and maintenance of Online Safety policies.
- Responsible for implementation of incident management protocols.
- Leads staff professional development in Online Safety knowledge.
- Liaises with outside agencies (e.g. Child Exploitation and Online Protection Centre [CEOP], Local Authority [LA]).
- Ensures that the technical infrastructure is in place, maintained and updated to support Online Safety (e.g. firewall, backup, Internet monitoring, filtering systems).
- Stays up to date with technical trends and issues concerning the ICT infrastructure and online access.
- Maintains CEOP Ambassador status with regular training.

Whole School Computing Coordinator (Ryan Perrens)

- Works with school staff on subject-specific issues regarding Online Safety (e.g., filtering of resource sites) and training needs.
- Ensures a uniform approach to Online Safety within the school.
- Encourages the development of online safety resources for use within the department.
- Responsible for coordinating Online Safety curriculum programme.
- Responsible for parental contact and information regarding Online Safety.
- Implementation of National Online Safety Resource across school and parents.

Heads of School, Associate Heads & Sixth Form Lead

- Ensures any instances of ICT misuse are dealt with in the appropriate manner.
- Supports the Online Safety Coordinator in the implementation of incident management protocols.
- Advises the Online Safety Coordinator on trends in students' ICT use that they become aware of.
- Develops and maintains a knowledge of current Online Safety related issues.
- Liaises with the Child Protection Officer on Online Safety related issues, when applicable.

Child Protection Officer (Liz Dean)

- Develops and maintains a knowledge of current Online Safety related issues, with particular regard to how they might affect vulnerable young people.
- Liaises with parents with any issues that relate to Online Safety matters.
- Develops procedures to support pupils who are identified by staff as needing support, as well as those who self-refer.

All Staff

- Implement the Online Safety policy.
- Develop and maintain a knowledge of current Online Safety related issues.
- Ensure Online Safety and copyright messages are reinforced in ICT lessons and activities.
- Check resources and links when planning ICT activities to ensure that inappropriate material is not inadvertently viewed.
- Report breaches of ICT security through the relevant channels.
- Maintain professional conduct when online, both inside and outside school.
- Ensure that any opportunities are taken to introduce online safety elements and justify reasoning.

Students

- Strive to uphold the Online Safety policy.
- Develop skills of critical review and working safely, both on technical and personal levels.
- Report any ICT misuse to a member of staff.
- Report any inadvertent viewing of inappropriate content to a member of staff.
- Seek help from an adult if they face problems.
- Discuss / educate parents / carers about Online Safety issues.

Acceptable Use

The school declares that all students and staff can use the ICT equipment for legitimate purposes, acting within a remit appropriate to their professional / student status, employ online safety practices consistently and follow procedures regarding Online Safety.

Staff are required to sign an AUP before being granted access to the school's ICT infrastructure and portable devices. AUPs are reviewed annually by the ICT Operations Manager to ensure that they are fair, up to date and take account of the latest technological advances and best practice from ICT advisory bodies.

Online Safety Education / Training

All ICT users are at risk of crimes such as cyberbullying, grooming, extremism, stalking and identity fraud through the illegal use of information and channels found online.
Students are taught:

- That there are many risks to disclosing personal data online.
- To carefully consider what personal information to put online and what it may be used for.
- About the consequences and impact of Cyberbullying and what to do about it.
- About the techniques some people employ to extract information for illegal use.
- Procedures when involved in Online Safety incidents, at home and in school
- How to ensure their personal data is kept safe from technological threats such as viruses, trojans.
- Not to trust information from unverified sources and unknown people.
- How to critically review and verify any information found online.
- About extremism and how online platforms can be used to radicalise.
- About copyright law, how it protects everyone, how to work within the law when collecting and using digital information.
- To teach relationships education, relationships and sex education, and health education.
- How to use technology safely, responsibly, respectfully and securely
- Where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Informal Teaching

It is important to consider that effective teaching of Online Safety skills in students is not simply a matter of “covering units”. All staff should be aware of Online Safety issues and build them into their teaching wherever possible, even as an informal class discussion. Advantage should be taken of students’ own experiences to discuss Online Safety with them.

For Students

There is a coordinated curriculum of Online Safety awareness:

- Primary – the core elements of Online Safety are covered at an appropriate level to ensure pupils are prepared for the dangers they could face online.
- Secondary/6th Form – students progressively learn more about Online Safety with more elements being introduced and further detail being added to core elements to ensure students have a solid understanding of all dangers and how to cope with them.

Within the school there are different Pathways and Online Safety looks different in each one, where possible it is expected to relate subject content to Online Safety elements/topics which helps support students understanding in and outside of the classroom.

The Online Safety curriculum is reviewed annually as part of normal scheme reviews.

For/Guardians

This document is available for parents on the school website. This ensures that Parental information is on the school's ICT provision, expectations of students and that Online Safety is shared within the school

Parent workshops are carried out to highlight the dangers and illustrate the correct procedures followed in school and how these can be used at home.

The resource of National Online Safety has been purchased and is available to all parents to help support their child outside of school.

Staff

New staff are trained in Online Safety matters as part of the induction programme. In addition, support and guidance are available from the Online Safety Coordinator.
For existing staff, Online Safety training is delivered annually as a standalone session and is also incorporated into the whole-school INSET programme as part of the Child Protection training.

The staff curriculum is based on the programme delivered the students, covering the same points. In addition, staff are trained on classroom management techniques to minimise risks to students and themselves.

The resource of National Online Safety has been purchased and is available to all staff to help support them in and outside of school.
Assessment
Assessment of Online Safety education and policy effectiveness is conducted as an integral part of their education. Students are taught about the subject at least once a year and work is assessed and feedback is given to reinforce understanding and knowledge.

Classroom

Whenever ICT is used in the classroom, all adults need to be aware of the potential for Online Safety incidents and breaches of ICT security. To minimise the risk of Online Safety incidents, staff should all adhere to the following classroom management protocols concerning Online Safety.

Always research web links before a lesson - can a student easily find themselves on inappropriate materials in a few clicks from your recommended site? Is all material suitable for the age range of the students?

Be active in all classrooms and do not allow unsupervised use - tour the room, looking for signs of secrecy. This normally means some illicit activity going on.
Be aware of phrases being used like LMIRL (Lets meet in real life) ASL (Age, sex, location), and students using web-based chat facilities (which should be blocked anyway).

If an incident occurs, determine its severity rating:

- **Minor** (games, emailing, general web surfing, storing / viewing images in the “silly” category)
- **Major** (viewing / storing / printing legal pornography, distasteful material, cyberbullying)
- **Extreme** (viewing / storing / printing illegal pornography, scenes of extreme violence, rape, torture; criminal activity such as fraud, hacking)

Follow the appropriate action in the Classroom Management section of this document. Please note the importance of not allowing anyone to use the computer after an extreme incident - police / CEOP may wish to check the computer for evidence. DO NOT attempt to email, re-view or print the content, as this is an offence in itself.

Students use e-communications facilities (email, instant messaging, texting, Twitter, blogs, YouTube, social networking sites) as part of their everyday lives.

You should ensure that you keep yourself safe by:

- Not divulging personal information online.
- Carefully managing social networking profiles.
- Using ONLY the facilities provided by the school to communicate with students and parents / guardians - DO NOT use personal email or other unauthorised methods.
- Considering your position as a professional, acting accordingly when online.

Protection of personal data

Students undergo an Online Safety lesson throughout the academic year, part of this covers protection of personal data.

Students are reminded about the importance of protecting personal data through discussions, posters or presentations.

The school's network filtering systems are configured to prevent student access to many of the sites which pose risks in terms of students posting personal data. (These include Facebook, Instagram etc)

Staff are required to adhere to the mobile phone policy, which reminds staff that posting personal data/information on social networking sites or using instant messaging services may put them at professional and personal risk.

Publicity (Photo / Video of Students)

Uploading images to online public systems

Since the school's website is a publicly accessible source of information, information must be carefully checked to ensure it complies with Online Safety standards before publication (decency, non-identifiable students etc)

All materials for web-site publication are reviewed and approved by the ICT Operations Manager/IT Team before being uploaded.

No material should be added to any public-facing information source (including the website) without approval by SLT.

Photography / Images / Videos

Students have their personal photographs taken for inclusion on the school's system. They are only to be used for this purpose and assessment walls, but must not be copied to shared areas, staff folders.

Students are at risk of identification if photographic images or videos are publicised along with name data. Care should be taken that no photographs / videos of students in combination with names are available on any public system.
It is preferable to publish group photos rather than individuals.

Care should also be taken to ensure that, in informal settings (e.g. school trips) the same standards of privacy, decency and non-identifiability are adhered to.
Before photographing / videoing any student in scenarios that may be publicised, you must refer to the photo list on Arbor

Incidents

Incidents concerning breaches of ICT security or cyberbullying will fall into several classes of severity. A definition of these, and the actions to be taken, are given in the subsections below.

For all incidents of Online Safety an entry should be made on our incident recording system CPOMS with the relevant category selected (Online Safety) and a description of the event including the severity of the incident.

Minor

Minor incidents (such as using personal devices during lessons) should result in the equipment (if mobile/personal) being confiscated and the matter referred to the form tutor, head of year or Online Safety coordinator.

The Online Safety coordinator will evaluate the incident for evidence of modifications needed, and will liaise with the relevant managers as appropriate.

Form tutors and heads of year will deal with the incident under the school's discipline procedures.

Moderate

Moderate incidents (such as: viewing or saving pornography / other offensive material, Cyberbullying by texting, emailing, taking unsolicited photos / videos) should be referred to the Online Safety coordinator and heads of year through the normal channels.

The SLT member will evaluate the incident and ask for any relevant evidence to help review the situation.

SLT will deal with the incident under the school's discipline procedures.
The IT Department will be responsible for providing evidence from the monitoring system.

Extreme (illegal)

Extreme incidents (such as viewing or saving of illegal material or activity such as fraud, hacking) have criminal implications and the procedure below must be followed immediately such an incident is discovered:

Upon Discovering the incident

For extreme incidents, the device should be isolated immediately from all users, screens turned off and the ICT Operations Manager and Online Safety coordinator informed immediately.

The password for the user concerned will be changed to lock down the machine to preserve evidence.

The Online Safety coordinator or child protection officer will notify the appropriate agencies (LA / CEOP / Police) for further advice.

It is VITAL that any ICT equipment used to commit an illegal act is not tampered with in any way, to preserve evidence.

The Lead IT Technician will produce a report of the incident to the Executive Head Teacher and liaise with staff on preserving evidence.

SLT will review impact of security breach on current Online Safety policies.
The Executive Head Teacher will liaise with the appropriate external authorities (Police / CEOP / Internet Watch Foundation).

Throughout this procedure, reference should be made to the "Appendix " flowchart "Flowchart for Responding to Online Safety Incidents", from NetSweeper publication Online Safety: Developing whole-school policies to support effective practice

Incidents implicating Staff

Extreme incidents involving staff should be dealt with using the same protocols as students.

Generally, the Executive Head Teacher will take the lead in incidents minor / moderate severity, liaising with IT staff, as necessary.
Once evidence has been collected, the school's Disciplinary Policy will be implemented.

Accidental viewing of inappropriate content

Students

Students should report the incident to the nearest member of teaching staff.
The teacher should then notify Lead IT Technician who should lock the appropriate machine and user account and use the monitoring software to provide evidence of the security breach.

The Lead IT Technician will then notify the Online Safety coordinator and SLT, and will review the security breach.

It is important that students feel supported and not criminalised in this instance, as doing so would dissuade them from reporting incidents of this type, with the consequent risks of further security breaches later on.

Staff

Staff should follow the above procedure if they accidentally view inappropriate content from within school. The procedure will be the same, but the Lead IT Technician will report the matter to the Head Teacher rather than Heads of Department.

Creating a safe

The school will employ such technologies and policies as it sees fit to ensure the security of:

- ICT infrastructure (e.g. virus protection).
- Protection against data against loss / corruption (backup strategies).
- Protection of personal data against unauthorised publicity, transfer, and use.
- Users against being exposed to inappropriate / damaging material.

Filtering

The school employs 2 levels of internet filtering system:
1. ISP - filtering. This is provided as part of the online connectivity package. The system is configured by Link2ICT with some guidance from our ICT Operations Manager (Online Safety coordinator). This provides customisable filtering.

2. School level filtering. Using the NetSweeper Client Agent, staff can request additional filtering of websites. The Lead IT Technician manages and implements changes.

Staff can request for filtering to be applied to ensure the school adapts to the changing dangers posed by the internet. Conversely staff can also request the removal of certain filters to allow them to access resources they require for a lesson. In this case it is carefully considered by the Online Safety coordinator in consultation with other members of the IT team.

Monitoring

Students and staff's online activities are monitored using the NetsupportDNA and NetSweeper system. The monitoring software is used in active mode, with the detection of key words resulting in the logging of the event and notification of the Online Safety Co-Ordinator. In the event of an incident being escalated, NetsupportDNA/NetSweeper can also be consulted later for evidence which is then supplied to the appropriate member of staff dealing with the incident. The monitoring system observes any activity on a user's screen and captures screen shots when specified words are detected on the screen. This can then be used as evidence in the event of an incident.

Anti-Virus / Firewall

The school subscribes to the ISP provided Anti-Virus package. Automatic updates are set to operate on all end-user workstations, laptops and file servers.
Laptops are protected by the Anti-Virus package even when offline.
The school employs ISP firewalls and uses on-site firewalls were deemed most appropriate.

Patches and updates to programs and operating systems are regularly applied to ensure security integrity is always maintained.

The school does not allow any unauthorised devices to be connected to its networks or other ICT Infrastructure. Wireless networks are encrypted by default, with security details known only to the relevant technical staff.

Social Networking Or mobile devices

There are specific school policies for Social Networking and Mobile devices. A summary of key points follows below.

Students

Social networking sites and newsgroups will be blocked unless a specific use is approved.

Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include their real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests, and clubs etc.

Pupils and parents will be advised that the use of social networking outside school may will be inappropriate for students aged 13 and below.

There is to be no communication with staff members in or outside of school, unless there is circumstance where this is not possible, e.g. School Trip, Residential, and Emergency Situation.

Communication with other students outside of school hours should be monitored by parents. If a situation arises with such as bullying the e-safety coordinator, Head of Year or Executive Head can be contacted.

Staff

Staff must never give out their personal details to pupils or parents.
Communication with other staff members outside of school via social networking is the responsibility of the end user. However, references to school and staff, students or parents, if of an offensive nature, may be subject to disciplinary investigation. Staff must be aware that anything posted on-line is in the public domain and may potentially be seen by anyone including non-intended recipients.

Communication with current students or parents, such as having them as a friend on social media, and messaging is not allowed by school. Uploading or sharing photos or videos with students in is also forbidden.

All staff must be aware that the posting of inappropriate pictures, videos and comments may be viewed as bringing the school into disrepute by association, which could be considered a disciplinary issue.

Staff must not share their contact details with current students or parents unless agreed by SLT. We also advise that staff do not share their contact details with past pupils or parents as there is usually still a link to school through current pupils and parents.

Any issues or queries need to be highlighted to the Online Safety Coordinator or Lead IT Technician.