



## WROTHAM SCHOOL

# E-Safety and E-Learning Policy

### Document Review

<b>Governors approval Date:</b>	<b>18<sup>th</sup> March 2021</b>
<b>Committee Responsible:</b>	<b>Local Governing Body</b>
<b>Next Review Date:</b>	<b>Mach 2024</b>

### *Equality Statement*

Wrotham School promotes equality of opportunity. We are committed to take a positive stand to ensure all stakeholders have a right to equality of opportunity and achievement regardless of race and ethnicity, faith, belief and religion, disability and access, age, gender identification, sexual orientation, and marital status.

Equality of opportunity is related to all areas of the schools work and is a fundamental aspect of the ethos of the school.

**Introduction:**

Wrotham School believes that the use of information and communication technologies in Schools brings great benefits when used safely and productively.

This e–Safety Policy is part of the ICT and Safeguarding Policies and it also relates to other Policies including those for behaviour and anti-bullying.

The e–Safety Policy and its implementation will be reviewed annually.

Our e–Safety Policy has been written by the School, building on the KCC e–Safety Policy and Government guidance. It has been agreed by the Senior Leadership Team and approved by Governors.

**School’s Designated Child Protection Coordinator:       Michael Cater**

**School e-Safety Coordinator:                   Paul Kitney (Network Manager)**

**E-Safety/Safeguarding Governor:                               Sheila Smith**

The rapid developments in electronic communications are having many effects on society. It is therefore important to state what we are trying to achieve in education through ICT and Internet use.

**Statement of Aims:**

At Wrotham School we aim to offer an IT and online network that is beneficial to students, parents, staff and visitors in learning, experiencing and staying safe and secure. The use of IT in School, when learning and in its extended communications with stakeholders, aims to improve and move forward the work we do as an educational institution underpinning our high expectations of everyone involved.

This policy is both a set of clear expectations, a guide for the School community and a source of information to improve e-Safety at the School and in wider experiences.

If you have any concerns regarding this Policy or other aspects of e-Safety at Wrotham School, please contact us using the details provided above or contacting [support@wrotham.kent.sch.uk](mailto:support@wrotham.kent.sch.uk).

The following is a list of online locations linked directly to the School. Information and resources on these sites is officially monitored and controlled by the School:

### **Wrotham School Online:**

<a href="http://www.wrothamschool.com">www.wrothamschool.com</a>	<b>School Website</b>
<a href="http://www.facebook.com/wrothamSchool">www.facebook.com/wrothamSchool</a>	<b>School Facebook Page</b>
<a href="https://wrothamSchoolsixthform.wordpress.com/">https://wrothamSchoolsixthform.wordpress.com/</a>	<b>Sixth Form Website</b>
<a href="https://wrothamrevision.wordpress.com/">https://wrothamrevision.wordpress.com/</a>	<b>Revision Website</b>
<a href="http://charactereducationtrust.org.uk/">http://charactereducationtrust.org.uk/</a>	<b>MAT Website</b>

To ensure this policy is clear and easy to reference, we have divided it into key aspects of e- Safety and described our objectives and expectations in regard to each element:

## **GENERAL**

### **The Internet**

- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The School will endeavor to ensure equality of access by providing supervised ICT out-of-hours access to all students.
- The School's Internet access is designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The School will ensure that the copying and subsequent use of Internet derived materials, by staff and pupils, complies with copyright law and exam and assessment regulation.
- Internet and online access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Students and parents will agree to a School based code of conduct that ensures safety and security through active and responsible use of the internet.

- Regular assemblies and progress time resources will be delivered to update students on key and current internet safety risks and strategies.
- An annual Parent e-Safety presentation will be held to inform and keep parents up to date with strategies for managing their children's safety online.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. It is the class teacher's responsibility to ensure students are guided in this process.
- The evaluation of online materials is a part of teaching/learning in every subject and forms part of the planning and preparation process.
- Images of a pupil will only be published for an appropriate reason and with signed consent from parents in the School's admission booklet.
- Images of a student, staff member or member of the public will be immediately removed from any of the Schools online publications as requested.

## **The Network**

The Schools Broadband network includes a cluster of high performance firewalls at each of the Internet connecting nodes. These appliances run industry-leading software and are monitored and maintained by a specialist security company.

The security of the School information systems and users will be reviewed regularly. Virus protection will be updated regularly.

Staff will be responsible for the safe-keeping of portable media AND ensuring reasonable steps are taken to protect and secure contents – e.g. 2 level password protection.

Unapproved software will not be allowed in pupils' work areas or attached to email. Files held on the School's network will be regularly checked.

The ICT Coordinator/Network Manager will review system capacity regularly.

## **DATA PROTECTION**

### **Data**

From 25<sup>th</sup> May 2018 the School will be fully GDPR compliant.

The quantity and variety of data held on pupils, families and staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 2018 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1918.

## **USEFUL RESOURCES, LINKS AND ADVICE**

Links and resources for online safety advice (*these can also be found in direct links from our website*):

### **CHILD SAFETY ONLINE**

[http://www.wrothamSchool.com/wp-content/uploads/2017/01/Social\\_Media\\_Guidance\\_UKCCIS\\_Final\\_18122015.pdf](http://www.wrothamSchool.com/wp-content/uploads/2017/01/Social_Media_Guidance_UKCCIS_Final_18122015.pdf)

[http://www.wrothamSchool.com/wp-content/uploads/2014/10/online-safety-checklist-pdf\\_wdf101283.pdf](http://www.wrothamSchool.com/wp-content/uploads/2014/10/online-safety-checklist-pdf_wdf101283.pdf)

[http://www.wrothamSchool.com/wp-content/uploads/2014/10/teenagers-checklist-pdf\\_wdf101287.pdf](http://www.wrothamSchool.com/wp-content/uploads/2014/10/teenagers-checklist-pdf_wdf101287.pdf)

### **MOBILE DEVICES**

<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/>

### **PORNOGRAPHY**

[http://www.wrothamSchool.com/wp-content/uploads/2014/10/onlineporn-checklist-pdf\\_wdf102634.pdf](http://www.wrothamSchool.com/wp-content/uploads/2014/10/onlineporn-checklist-pdf_wdf102634.pdf)

### **THINK YOU KNOW**

<https://www.thinkuknow.co.uk/>

### **PARENT CONTROLS**

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/parental-controls/>

### **CHILD NET**

<http://www.childnet.com/>

## **ONLINE ABUSE**

<https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/>

## **SOCIAL NETWORKING**

<https://www.net-aware.org.uk/>

## **INFORMATION FOR STUDENTS, PARENTS and STAFF**

### **For Students**

We actively work to improve student's online safety by:

- Running regular assemblies and PSHE days focussing on online safety.
- Information and discussions during Progress Time.
- Work with the local police force to educate and support students in reporting online crime.
- Keeping up to date with changes in trends and technology that change the way student's access online entertainment, interaction and information.
- Training staff on internet safety and responsibility.
- Providing suitable sanctions for any student that behaves unacceptably online.
- Ensuring that all devices in School are monitored and restricted appropriately.
- Information evenings for parents.
- If you have any further questions or concerns regarding your child's online safety please contact Mr M Cater, Headteacher.

With an increasing amount of communication being conducted online it is important that we make our expectations in this area clear. The most important element of our work is to ensure students are safe online and that they conduct themselves to the same high standards expected in other areas of their lives.

- Students are encouraged to speak openly about their online experiences and report anything that they feel uncomfortable about. They should not feel scared about speaking to a trustworthy adult if they have any concerns.
- Parents and students ask the School for help in managing their child's online behaviour.
- It is made clear what is "acceptable" and "unacceptable" online behaviour.
- Parents inform and work with the School when online behaviour risks impact on School life.
- Access to the internet, gaming and social networking is monitored and reasonably limited so that students do not lose sleep, homework time or become unhealthily distracted by it.

**We will not tolerate or accept:**

- Bullying or intimidating of others online using phones, social networking sites and apps. This includes Racist, Sexist, transphobic or homophobic messages, statuses or comments made online in any context.
- The publishing of anything online that may unfairly bring the School into disrepute.
- Public discussion about School matters or incidents online that involve others.
- Any behaviour online that is considered slanderous, illegal or would not be accepted in School.

**Mobile Phones**

Mobile phones are internet enabled devices and the same rules and guidelines are applied to their usage in School.

If brought in to School these must be switched off during School hours and kept safely with personal belongings. Students are not allowed to use mobile phones during the School day from 08:30- 3:05.

If parents have to be contacted this must always be done using the School telephone, with the permission of a member of staff. For the safety of your child please only communicate with the School office.

Students seen using their mobile phones during the day will have them confiscated and returned at the end of the day. The School will not accept any responsibility for loss or damaged mobile phones when used on the School site.

**Student Code of Conduct**

- I know that I must use the computers safely.
- I will only use my own login and password which I will keep secret.
- I know that the School remotely monitor what I do on the computers.
- I will be aware of my personal safety when I am communicating online and will not share personal information about myself or others.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer or anything that makes me feel uncomfortable when I see it.
- I know that I must use the computers responsibly.
- I understand that the computers are here for School work and I will only play games on them or use them for personal use if I have permission.
- I will only upload pictures or videos from inside the School if I have permission.
- I understand that the School's security and Internet filter is there to protect me and protect the computer network and I will not try to bypass it. If I need access to a blocked website, I will ask my teacher.

- I will only download music or videos onto the computer if it is related to my School work.
- I understand that I must not download or display inappropriate pictures or other material from the Internet. I know that I must help look after the computers. If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person.
- I will only use programs that are already on the School computer. If I need a new program, I will ask my teacher - I won't try to install it myself.
- I will not try to connect my own computer or mobile phone to the network.
- I will only change settings on the computer if I am allowed to do so – I won't try to change anything that might cause the computer to go wrong.
- I know that food and drink is not allowed in the computer rooms and that I should not eat or drink around any computer.
- I know that I must respect others when using the computers.
- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.
- I will be polite online and I will not use strong, aggressive or inappropriate language.
- I appreciate that others may have different opinions.
- I will not misuse photographic or recording devices to encroach on anyone's privacy.
- I will not take/ record or distribute images of others without their clear consent and I will ensure these images are appropriate and will not cause upset or distress.
- I take full responsibility for any image I record or take. This includes ensuring this image is legal, appropriate and is not distributed or published inappropriately

I understand that the School monitors the use of the computer systems, including the monitoring of websites, the interception of E-mail and messages. We will delete inappropriate material in circumstances where it believes unauthorised use of the School's computer system, is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

### **For Parents**

At Wrotham School we pride ourselves on our outstanding provision of E-safety learning.

Each year we provide regular and thorough information to parents regarding staying safe and positive behaviours online. As you will know, the online safety of our students is constantly changing and growing and ensuring we prepare young people for this world is one of our highest priorities.

The School asks that parents are up to date and aware of the changes to technology and usage. This is a responsibility of good parenting and it is imperative that they are aware of the dangers of unmonitored online activity.



We continue to deliver our assemblies, classroom activities and parent information evenings to ensure we keep everyone up to date and well equipped to navigate the pitfalls and dangers of new technology in a balanced and measured way.

On occasion the Headteacher will write to parents to politely request your support and commitment to helping us keep your children safe online. The information does not intend to tell you how to parent but hopefully provides useful support and advice to help us keep children safe.

In recent years we have seen a rise in online bullying both towards and by young people. This abusive behaviour is mostly seen on Instagram and Snapchat but can extend to other social networking applications. Much like traditional “playground bullying” this leads to name calling, social exclusion and threats or intimidation.

Many issues can be avoided through support at home and the monitoring of students behaviour online, at home.

We request that parents take an active role in monitoring their child’s interactions online. This includes the use of mobile phones, social networking sites and the internet in general. As parents and teachers we have a responsibility to understand the world our children live in and do our best to learn from them about what they are doing and why.

### **Advice for Parents:**

- Students, particularly in years 7-10, should not be allowed to use Apps/Sites such as Instagram or Snapchat without full parental access to passwords and accounts.
- Students should not befriend anyone they do not know or they are not friends with. We often find students are “online friends” with the same people who are bullying them.
- The same rules that apply in society and by law apply to online behaviour. Students who break these laws risk prosecution. This includes online harassment, hate speech, racism and homophobia, even when this is in “private conversations”.
- Students should not engage with online bullying or abuse of others and should block anyone who they feel is being abusive.
- Be aware of duplicate or extra devices such as second phones, online games consoles and smart TV’s which can access the same online content even after confiscating a mobile phone.
- Internet access and access to mobile phones should be removed overnight to prevent disturbance to sleep and unhealthy, unmonitored access to these sites.
- Students should be able to share their online comments and messages with you as their parent, openly. This is not a matter of privacy, but of safety. If a young person is secretive or resistant to sharing this, there is likely to be something wrong.

- Most importantly issues of abuse and bullying online from other students, young people or adults should be reported to the School using our pastoral system, form tutors, heads of School and safeguarding team. We will always ensure our students are kept safe.
- The School will inform parents/carers of any incidents of concerns as and when required.
- The School is available to answer any questions and offers annual e-Safety events to ensure that parents are supported in learning about these changes.
- Parents' attention will be drawn to updates to the School e-Safety strategy in newsletters and on the School website.
- Parents will be requested to sign an e-Safety/Internet Agreement as part of the Home School Agreement.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
- Advice on e-Safety and links to verified websites can be found on our School website and offer further reading and support for parents when managing their child's safety online.

### **Mobile Phones**

Mobile phones are internet enabled devices and the same rules and guidelines are applied to their usage in School.

If brought in to School these must be switched off during School hours and kept safely with personal belongings. Students are not allowed to use mobile phones during the School day from 08:30- 3:05.

If parents have to be contacted this must always be done using the School telephone, with the permission of a member of staff. For the safety of your child please only communicate with the School office.

Students seen using their mobile phones during the day will have them confiscated and returned at the end of the day. The School will not accept any responsibility for loss or damaged mobile phones when used on the School site.

### **For Staff**

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of School. However it is also important to consider the risks associated with the way these technologies can be used.

Staff should develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered

jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the School Designated Child Protection Coordinator.

The Designated Child Protection Coordinator must be informed of any e-Safety incidents. The School will manage e-Safety incidents in accordance with the Safeguarding and School Discipline/Behaviour Policy where appropriate.

Where there is cause for concern or fear that illegal activity has taken place or is taking place, then the School will contact the Children's Safeguarding Team or e-Safety Officer and escalate the concern to the Police.

After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes required.

## **For Staff**

### **Wrotham School - Staff Code of Conduct for ICT**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct.

- I understand that it is a criminal offence to use a School ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobiles phones, PDA's digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for School businesses.
- I understand that School information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my School information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in School, taken off the School premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and make every reasonable effort to ensure that these communications cannot be misunderstood or misinterpreted. I will ensure that I only communicate with students using the official Wrotham School email.
- I will promote e-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will ensure the content I publically publish online, including posts and content, written or endorsed by me on social networking sites such as Twitter and Facebook in no way brings myself as a professional, the School or the teaching profession into disrepute.
- I will ensure that I take all steps to make personal data and online profiles private and secure. Staff must not link, friend, follow or add pupils currently at Wrotham School or former students under the age of 18. Staff should be aware that their online activity may be seen by students who have mutual friends or links. (This also applies to other social networking sites).
- I will ensure that my behaviour online reflects the equivalent published behaviours expected by the current professional guidelines that relate to teachers conduct.
- It is the responsibility of individual staff members to understand how independent online services such as Facebook or Twitter work. If an individual does not fully understand how to manage their privacy or online footprint the School recommends they avoid using these services.

The School may exercise the right to monitor the use of the School's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

### **Wrotham School – Staff Email and Communications Etiquette**

This document outlines the Schools expectations of email and electronic message protocol to ensure fluid, productive and appropriate communications in and out of School using the Schools email servers and contact addresses.

Emails and electronic communication can be a huge time saving device and can be highly useful communication tools. They should be used, where possible to communicate effectively and reduce workload.

This guide has been developed through consultation with staff and is intended as a guide to good practice that is conducive to healthy work/life balance and professional standards.

- All emails and communications should be succinct and to the point. They should not take excessively long to read or write.
- Emails and communications regarding work should only be sent or replied to between the weekday hours of 8.00 and 19.30. On weekends emails should only be sent between the hours of 10:00- 16:00 on Saturday and Sunday. There is no obligation to reply to any email after 18:00 on weekdays or on weekends. This includes emails from parents.
- We strongly recommend not replying to parental emails after 19:00 each day or at the weekend. This can lead to unrealistic expectations for other staff.
- Emails sent outside of this time should be sent with delayed delivery or saved as drafts so they arrive during the recommended hours.

- Urgent communications outside of these hours should be made via phone call, only if absolutely necessary.
- Staff should be aware that the tone of emails can be misinterpreted and that sensitive conversations should be had in person to avoid risk of misinterpretation.
- School email accounts must not be used for personal communications.
- Emails to parents or in response to staff requests should be responded to, if requested, within 48 hours or ASAP for serious or safeguarding concerns.
- Emails should be checked for spelling, punctuation and grammar and should be suitably checked for the intended recipient. There is a difference between informal and formal emails.
- Emails sent from/at work are monitored periodically and emails sent using the School email system may be monitored by the Leadership team of the School to maintain safeguarding and professional standards.
- Confidential emails must be identified as such in the header of the email.
- Student initials should be used in the header of an email to ensure that confidentiality is not breached. Where possible names or initials should not be used in the headers of emails.
- Attention must be given to who receives or is copied into an email. All staff should only be emailed when the content is relevant to all staff. Groups or individuals should be identified and addressed to ensure unnecessary emails are kept to a minimum.
- Good communication with parents is important. If you are unsure of how to respond to a parental email please consult with a member of the Leadership team before replying.
- Email communication with students should always be using a School email account and content should reflect appropriate and professional standards.