WOODBRIDGE HIGH SCHOOL

Acceptable Use Policy and E-Safety Guidance for Staff

Updated: September 2018

Name of organisation:	Woodbridge High School
Designated Officer:	Jeremy Clifton
Deputy Designated Officer:	Faheem Khan

Please sign below once you have read and understood the terms of the following policies:

- *E-safety policy*
- *Acceptable Use Policy*
- *Digital Technology Handbook*
- *Data Security Policy*

Print Name _____

Signed _____

Date _____

Acceptable Use Policy for Staff

Internet access: You must not access, or attempt to access, websites that contain or promote any of the following: extremism and radicalisation; child abuse; pornography; discrimination of any kind; racial or religious hatred; illegal acts; any other information which may be illegal or offensive to colleagues. It is recognised that under certain circumstances inadvertent access may happen. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Leadership Group so that it can be logged.

Inappropriate/Illegal content: Access to any of the following should be reported to the Police: images of child sexual abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 18 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK. Access to extremist material must be reported to a Prevent officer.

Social networks: Members of staff should never knowingly become "friends" with children on any social networking site or engage with children on internet chat.

Communication: All members of staff should use their school email address for conducting professional business. This includes communications with parents and students. Any information pertinent to the school record should be stored away from mailboxes. Any official communication is potentially disclosable and if it cannot be justified is liable for legal action on a personal level.

Remote Access: Staff are permitted access to their school documents using the secure remote desktop protocol (RDP). Please ensure full compliance with data protection and do not leave your home computer unattended when logged in.

Passwords: Keep your passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection: Where a member of staff has to make use of personal data, sensitive or confidential information outside of school environment, sufficient safeguards should be in place to mitigate the risks of loss or misuse. Staff must use remote desktop to access such information from the home environment. Staff must not use USB sticks to transfer sensitive and confidential information. All data relating to staff, students and parents must be kept private and confidential.

Personal Use: Staff are not permitted to use ICT equipment for personal use without Leadership Group approval. If personal use is permitted the boundaries of use should be written down and adhered to.

Images and Videos: No images or videos showing a student should ever be uploaded to a website or social network without the express permission of parents or the child's carer. Similarly no personal information (name, date/place of birth, mobile number, email address etc.) should ever be shared.

Use of Personal ICT devices/Bring Your Own Devices (BYOD): Use of personal ICT equipment (i.e. mobile phones, cameras, personal laptop etc.) is at the discretion of the Leadership Group. Any such use should be stringently checked for up to date anti-virus and malware checkers. Use of personal ICT devices is subject to the same Acceptable Use Policy. Pictures or videos of children must never be taken using personal ICT devices.

Reporting concerns: It is the duty of staff to support the school's safeguarding policy and report any behaviour which is inappropriate or a cause for concern to the appropriate authority. Incidents involving students: report to designated child protection officer. Incidents involving staff: report to the headteacher.

Monitoring: Emails and internet activity are subject to monitoring.

Woodbridge Digital Technology Handbook: This is a comprehensive overview of all ICT–related matters. Staff should read this carefully in order to be well-informed and compliant with school policy.

Policy Prepared by: Mr J. Clifton, Deputy Headteacher, and circulated in draft form: September 2018

Recommended to the F&GP Committee for approval on 10th October 2018

Date of Next Review: September 2019