I3. STAFF AND PUPIL ICT ACCEPTABLE USE POLICY

Our mission is to develop happy, confident and successful children who are well prepared for their future.

ISSR no.	N/A
Policy Owner	Deputy Head Pastoral
Reviewed by Deputy Head Pastoral	14.03.25
Reviewed by Headteacher	17.03.25
Reviewed by Governing Body	25.03.25
Renewal date (by)	31.03.26

SCOPE OF THIS POLICY

This policy applies to all school computers used in school, and also online behaviour, both inside and outside of school.

In addition to 'desktop' computers, this policy covers but is not limited to, all devices listed below (referred to as 'devices'):

- Mobile telephones;
- Laptops including chromebooks, both school and pupil owned;
- Tablets;
- Wearable Technology (e.g. Smart watch);
- Digital recording devices;
- Digital cameras;
- Mobile games consoles.

The facilities offered by the Local Area Network (LAN) at Westbrook Hay are available for use by all staff and pupils. This policy applies to the use of all school owned or managed devices as well as personal mobile devices used to communicate with, to or about Westbrook Hay or members of the school community. This policy is an extension of the school rules and employment laws and any breach will be dealt with through the usual channels (please refer to the Disciplinary policy for staff or Behaviour policy for students).

This policy is for all staff (to include Governors), visitors and pupils and is implemented to protect the interests and safety of the whole school community. It is linked to the following school policies:

- Child Protection and Safeguarding Policy
- E Safety Policy
- Anti-Bullying Policy
- Behaviour Management Policy
- Staff Behaviour and Disciplinary Policy
- Bring Your Own Device Policy
- Taking, Using and Storing Images of Children Policy
- Social Media Policy
- GDPR Privacy Policies.
- KCSIE 2024
- AI Policy

USER RESPONSIBILITY

Use of any devices shall be in line with this policy which each individual (or for younger pupils, their parents) are required to read and sign to say they (or their child) will abide by it before being granted access to the school network.

Westbrook Hay accepts no responsibility for the safeguarding or replacement of personal devices which are lost, stolen or damaged. It is recommended that individuals take out their own insurance for all such devices.

USE OF DEVICES

In line with EYFS regulations personal mobile devices (including wearables) are not allowed in the EYFS setting. Please refer to the BYOD policy for more details. Pupils are not permitted to have a personal mobile device (including wearable technology) in school without the express permission of the Head Teacher.

School mobile devices must never be used in changing rooms or toilets or when moving about the school campus regardless of the time of day / day of the week.

Mobile devices/tablets may only access the internet via Pupil Wi-Fi; 'hot spotting' is not allowed.

USE OF AI ENABLED SOFTWARE

The use of AI-enabled software is permitted within the school, subject to the following guidelines:

- Pupils may not use AI-enabled software to impersonate others or engage in any activity that may be considered deceptive or malicious.
- Pupils may not use AI-enabled software to cheat or gain an unfair advantage in any academic task. Specifically, this means not submitting AI-created content without the necessary references or acknowledgments.
- Pupils must be aware that teachers may use AI-enabled software to assist with marking.
- They will be informed in advance of any instances where this will occur. Teachers will always review the accuracy and integrity of AI-enabled marking.
- Pupils must follow age restriction rules for personal accounts and must otherwise use AI-enabled software under adult supervision.

ONLINE BEHAVIOUR

It is forbidden to use the school network to access, create or send material, which is offensive in the normal context of a school, or in breach of the law.

It is forbidden to distribute information about a third party / member of the school community without their permission. It is forbidden to publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.

Electronic communication between staff and pupils must only be part of approved school activities, and only via approved forms of communication (School email, Intranet, Google Classroom et al).

Any individual caught using a mobile device to cheat in examinations or other formal testing opportunities will face disciplinary action In public examinations, this may also be reported to the examination board in line with The Joint Council for Qualifications malpractice guidelines

Report any suspicious online sexual approaches or threatening behaviour to your Form Tutor, Pastoral Lead, Head of Section or any trusted adult at school (pupils) and to the authorities where appropriate. Staff should always log concerns raised by pupils on RecordMy so that the DSL is aware.

The school may, at any time and without further notice, monitor pupils' use of IT systems and online behaviour to maintain safety and compliance with this policy.

It is not permitted to share passwords or log on details for accessing the school network. Always ensure that personal mobile devices are clearly named and have passcodes enabled.

Electronic devices should not be used in any situation that may cause disruption to the school day, embarrassment or discomfort to fellow members of the school community to include pupils, staff and visitors to the school campus. For this reason, devices may not be used to audibly play music / media during the school day, without the express permission of a member of staff.

Users will also be held accountable for their actions when using any aspect of the school IT system, whether at school or from an external site, or when using the school as a context for the communication of electronic information (e.g. publishing a website from home which may involve reference to the school, its staff or pupils). This includes keeping passwords secure to prevent unauthorised

access to the school Google Drive, SchoolBase and e-mail.

BEHAVIOUR EXPECTATIONS

What individuals do or say online is covered by a number of laws. Staff must reflect carefully on what they are posting online. Up to date guidance can be found here:
https://www.report-it.org.uk/reporting_internet_hate_crime#:~:text=While%20you%20may%20come%20across,is%20committed%20with%20hate%20motivationPupils

It is, at all times, forbidden to use any online or electronic method to send or publish offensive or untrue messages or post unpleasant comments/imagery that could intimidate, harm, or humiliate other users or their families and could also be breaking the law; this includes 'trolling'.

Individuals must not publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.

To this effect it is strictly against school policy to use a personal mobile device to video, photograph, upload, distribute, store or create material containing another member of the school staff without their express permission. A personal mobile phone should never be used to photograph or film a pupil.

Individuals should at no time use mobile devices to bully, harass, denigrate, post or distribute private information about a third party whether that be through the use of email, messaging, telephone calls, 'apps', Bluetooth, photographs or video images or social networking / blogging websites or any form of electronic or printed communication. If caught, individuals will face disciplinary action.

It is forbidden to use the school network to access, create or send material, which:

- is violent or which glorifies violence;
- is criminal, terrorist or which glorifies criminal activity (including drug abuse);
- is racist or designed to incite racial hatred;
- is of extreme political opinion, blasphemous or mocking of religious beliefs / values;
- is homophobic;
- could be construed as bullying or harassment;
- is vulgar, pornographic or with otherwise unsuitable sexual content;

- is crude, profane or with otherwise unsuitable language;
- is offensive in the normal context of a school;
- is in breach of the law including copyright law, data protection and computer misuse.

Any individual who is caught using vulgar, derogatory, racist, homophobic, profane or obscene language or imagery 'online' or where it has been deemed that this policy has been breached and that the material in question is causing harm or distress to another member of the school community, the individuals involved will face disciplinary action in accordance with school policies / disciplinary procedures.

Any individual caught using a mobile device to cheat in examinations or other formal testing opportunities will face disciplinary actions in line with those as laid down by the relevant examining body and in line with the school rules.

Further to the above users of the school LAN, or school / personal IT equipment or mobile devices must:

- not use other peoples' user identities (user names) or passwords, even with their permission or allow others to use their username or password (on any system);
- ensure any software installed on privately owned computers is properly licensed. (The school does not have any licensing agreement to cover such software);
- not attempt to gain administrative access to the School's network;
- not attempt to bypass any school system including but not limited to our internet filtering or Chromebook management tools;
- not enter into activities such as packet sniffing and port scanning. Reported occurrences will be treated as vandalism;
- not physically misuse or mistreat any piece of ICT equipment nor attempt to disrupt use by others or tamper with the system;
- report any suspicions regarding a virus to the IT staff immediately.;
- ensure devices are virus free, with antivirus software installed as appropriate. The owner of the device must ensure that updates / operating patches are applied to their device as they are released, any 'infection' passed into the network will be treated as a malicious act of vandalism if found to be the fault of the user.

Electronic contact and discussions between members of the Westbrook Hay

community must be respectful and professional at all times and communications between staff and pupils must only be part of approved school activities, and only via approved forms of communication (School email, Google Classroom, Zoom et al).

PROTECTING IDENTITIES ONLINE

Identity theft is an online danger that is increasing. It is strongly recommended that pupils/staff do not upload or reveal personal family or other Westbrook Hay users' personal details online (e.g. address, phone number, date of birth, financial details, passwords, etc.) Images that could cause embarrassment should not be uploaded. Uploading digital photographs taken from a mobile device may reveal precise GPS locations at a given date and time, and therefore may reveal personal movements and locations. It is recommended that pupils avoid using their photograph to identify themselves online, and use an avatar or cartoon image as a profile picture instead.

Unauthorised access to IT systems, accessing others' social networking accounts, email accounts etc., without their permission is an offence under the Computer Misuse Act.

REPORTING CONCERNS

Pupils should report any suspicious or inappropriate sexual approaches, messages or similar online behaviour to their parent or teacher; they may also report serious or urgent suspicions to the police by using the 'Child Exploitation and Online Protection' or 'CEOP button' available on many online chat & social networking sites, or seek help via the CEOP website.

All concerns should be logged on Record My for the attention of the Designated Safeguarding Team.

LOGINS

Logging onto the school network, mobile device, and/or any other school IT systems, forms an agreement to follow the guidelines and policies for ICT use at Westbrook Hay. Individuals are responsible for any activity that takes place using school logins or any other password protected system. passwords for the school network and any other online facility must be kept secret and must be changed regularly. IT support should be informed if there is suspicion that someone has obtained passwords.

Passwords should be difficult to guess and protected from view when entering. It is good practice to have different passwords for different systems rather than the same password for all. Pupils/staff should not log on to a computing device or any ICT system using another person's password, or use such devices or systems that have been left logged on. If moving away from workspaces, the machine should be locked using (windows key + L). At the end of a session, IT systems should be properly logged off.

CONSEQUENCES OF UNACCEPTABLE USE

Westbrook Hay will act strongly against anyone whose use of ICT could bring the school into disrepute or risk the work of other users; this remains valid even if the incident occurs outside of school. The consequences of misuse, abuse, illegal use or the breaking of any of the rules, as set out in this policy will be dealt with by the Headteacher or a staff member nominated on his behalf and could include referral to outside agencies such as the Police, as appropriate.

If the device is suspected of being used to bully, harass or transmit offensive material it may be searched by a member of staff, in accordance with the school's search policy; and this may result in the deletion of the offending material.

Should the infringement pertain to a Child Protection matter, the device will be handed directly to the Designated Safeguarding Lead who will log receipt of the device and act in accordance with the relevant school policy and advice from external agencies.

THEFT, ACCIDENTAL LOSS OR DAMAGE

All devices should make use of security features to ensure that should the device become lost it cannot be accessed by a third party; thereby eliminating the ability of a third party to distribute unsolicited information by pretending to be the owner of the device.

Pupils and staff are solely responsible for the safekeeping of their devices and should ensure that they are kept securely and clearly marked with the owner's name so they can be returned to their owner if found.

Items that are found and are not clearly marked or identifiable will be handed to the IT Manager. Pupils and staff will be made aware that such devices are held in lost property. Unclaimed / unnamed devices will be held in lost property for up to

and no longer than one term, they will then be disposed of.

Devices owned by the school (devices issued to staff or pupil loan devices) remain the property of the school and the loss of one of these devices may result in disciplinary action and/or the cost of the device may be billable to the user.

EMAIL

School email addresses are supplied to staff (for all work-related communication) and pupils. Staff should not use their work email address for any personal matters including, but not limited to signing up to streaming services or as a contact detail for utility bills. Staff personal email addresses must not be used to contact parents or pupils for any reason.

MONITORING & FILTERING

The welfare of pupils is of paramount importance; Westbrook Hay uses various technologies to monitor both internal and external Internet and e-mail traffic, whilst respecting privacy at all times. The School reserves the right to inspect data files and network logs if automatic detection of illicit content is triggered.

Manual investigation of email transmissions will only be carried out with the permission of the Head/Bursar.

The school uses third party software to block sites which are deemed age inappropriate or pose risks to pupils. Inevitably all such sites cannot be blocked however, the vast majority are and the filters are regularly updated and amended to prevent unacceptable media entering the school systems. We block all sites provided by The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) blocklists, per our requirements. Parents are encouraged to contact the IT staff if they have any concerns over the use of email or the internet by their child.

LIABILITY

Westbrook Hay accepts no responsibility for the safeguarding or replacement of personal mobile devices which are lost, stolen or damaged whilst on school property or during extracurricular activities, trips or when travelling to and from school on school transport. It is recommended that staff/parents/guardians take out their own insurance for all such devices

The school makes no guarantee, whether expressed or implied, for the information carried over the network or internet service it provides. Although the

systems offer a very high level of protection, the school cannot be held responsible or accept liability for any damage or loss of data, or the consequences of such damage or loss, whilst any member of the school is on the school system. The school accepts no liability for any damage caused by any type of computer virus, however it originates. The school accepts no liability in the unlikely event that damage is sustained to a privately-owned computer as a result of its being connected to the network or accessing any school systems.