THE WESTGATE SCHOOL

Hampshire's First 4-16 'All Through' School

"The Westgate School is a community of learners where partnerships inspire success for all: learning together – achieving excellence"

Headteacher: Mrs F A Dean, MA (Ed)

Initial Policy date	March 2015	Next scheduled review	May 2025
Governor approved	May 2024	Key person/people	Site & Facilities Strategic Lead
Model Policy		Model localised	Yes
Pupil leadership team review		~~Y / N /~~ N/A	

SAFE USE OF ICT AND OTHER DIGITAL DEVICES – FOR SCHOOL COLLEAGUES

Principles:

The Westgate School (referred hereon in as TWS) looks to enable the advantages of a wide range of ICT systems and other digital devices, both in school and outside of school. In doing so, TWS has a responsibility to ensure that ICT is used appropriately. Where this policy is breached, this may become a matter for Children's Services and/or a disciplinary issue. Colleagues should also be aware that this extends to any inappropriate use of ICT and digital devices outside TWS. This Policy applies alongside our Data Protection Policy.

This policy applies to the school governing body, all employees, whether employed directly by the school, or a third-party service provider.

This "Dos and Don'ts" list prescribes the types of behaviours and actions that colleagues should undertake to protect TWS and themselves from risk. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions colleagues should not display, or undertake as well as those that they should:

Practice and Procedures:

Do

- Ensure that your device is brought into school at least once every 2 weeks to be updated with anti-virus/securing software (happens automatically when you log in).
- Ensure that where a login and password is required for access to a system, it is not disclosed to anyone.
- Enable Multi-factor authentication when using email account(s) on non-school devices.
- Be aware that the school's systems will be monitored and recorded to ensure policy compliance.
- Ensure that you comply with the requirements of the Data Protection Act when handling personal data.
- Seek approval from your Line Manager before taking personal data off the school site.
- Ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely.
- Report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher, Designated Safeguarding Lead or Data Protection Officer as appropriate.
- Be aware that a breach of the School's Safe Use of ICT and Other Digital Devices Policy may be a disciplinary matter.

- Ensure that any equipment provided for use at home is not accessed by anyone else.
- Ensure that you have signed the Allocation of IT Equipment form confirming what equipment you have been allocated and that should your employment cease, all IT equipment will be returned in working order.
- Ensure that you seek support from the IT resource team with technical issues.
- Ensure that your use of ICT conforms to appropriate H&S regulations.
- Alert your Line Manager, Data Protection Officer or Designated Safeguarding Lead if you receive inappropriate content via email.
- Be aware that the school may intercept emails where it believes that there is inappropriate use.
- Alert the Headteacher if you accidentally access a website with inappropriate content.
- Use dedicated school mobile devices when on educational visits – not a personal device
- Ensure that your mobile device is switched off during lessons and meetings.
- Immediately report to the Headteacher/Designated Safeguarding Lead any occasion where a pupil has sought to become your friend through a social networking site.
- Follow school procedures for contacting parents and/or pupils. Only contact them via school-based computer systems, telephones or the School email system
- Take extra care when sending sensitive or confidential information by email, ensuring it is received by the intended recipient, only.
- Ensure that all School systems, devices, desktops, laptops are locked when they are left unattended.
- When teaching or delivering lessons online, for example through Microsoft Teams:
    a. ensure you continue to follow the same expectations of colleagues as within school (see Code of Conduct policy)
    b. remind pupils of expectations around behaviour (see Behaviour policy)
    c. delete any recorded lessons which contain pupil names, pupil 'chat', pupil voices or pupil images within one month – these should be used for catch up purposes only
    d. remind pupils, where appropriate, how to use their technology safely (see Digital Safety Strategy on the School Website for information)
    e. ensure your background is blurred or plain so pupils do not see into your home, and ask pupils to do the same if their cameras are switched on
    f. report any safeguarding concerns to the DSL as you would do normally (see Safeguarding policy)
    g. only communicate digitally with pupils and parents through your school email address or MS Teams
    h. ensure microphones are muted when not in use, to reduce the risk of background noise or overhearing of 'out of school' conversations
    i. continue to ensure Data Protection requirements are met (see Data Protection policy)

Don't

- Use School owned digital resources for personal use.
- Access or use any systems, resources or equipment without being sure that you have permission to do so.
- Share your login and password details with anyone.
- Download, upload or install any software or hardware (including USB sticks) without approval from the IT Support Team.
- Use any unsecure removable storage devices to store personal data.
- Use school systems for personal financial gain, gambling, political activity or advertising.
- Use personal email addresses to communicate with pupils or parents.
- Accept friendship requests on social media or online gaming platforms, or virtual reality platforms such as Meta from pupils or parents – you may be giving them access to personal information and allowing them to contact you inappropriately.

- Put information or images online or share them with colleagues, pupils or parents (either on or off site) when the nature of the material may be inappropriate or identify pupils.
- Post anything that may be interpreted as inappropriate towards colleagues, pupils, parents, the school or HCC.
- Accept friendship requests from former pupils within 2 years of leaving or until they reach 18, whichever comes first.
- Utilise social networking sites while at work.
- Use children's surnames during Online lessons
- Use personal text messaging accounts such as WhatsApp for official school business, for example: identifiable/personal information regarding a pupil, or employee
- School accounts such as O365, Teams is to be used for this type of correspondence to enable the school to manage a Subject Access Request in the event of this being received

Any breach of this policy may lead to disciplinary action. Depending on the severity of the situation, further action may be taken by the school or appropriate authorities.

It is important that this document is read in conjunction with other relevant School policies:

- Data Protection Policy
- School Social Media Policy
- Behaviour Policy