Information Communication Technology Acceptable Use Policy

Document Change History.

Version no	Date	Change made by	Brief details of change
1.0	*May 2000*		*Policy Produced*
1.1	11.10.23	Curriculum Committee	Filtering and Monitoring section added. Point no 5 amended to add in “server or email”. Point 3 added under “unacceptable use”. Header page updated. Footer added
1.2	27.11.25	Bursar	Section on AI added on page 5
1.3	20.03.26	Bursar	Paragraph re Mobile Phones added on page 6
1.4			
1.5			
1.6			

Document Review History.

Review Date	Reviewed by	Comments
June 2010		*Reviewed*
Sept 2019		Reviewed
11.10.2023	Curriculum Committee	Amended as per version 1.1 details
26.11.2025	Full Governors	Amended as per version 1.2 details
18.03.2026	Full Governors	Amended as per version 1.3 details

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the Internet or the school's Intranet will only be permitted upon receipt of signed permission and agreement forms as attached All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to Mrs Maysey or Miss Webster.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.

3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
5. Password – do not reveal your server or email password to anyone. If you think someone has learned your password then let Mrs Maysey know.
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Staff or students finding unsuitable websites through the school network should report the web address to Mrs Maysey.
10. Do not introduce floppy disks or "pen drives" into the network without having them checked for viruses.

11. Do not attempt to visit websites that might be considered inappropriate. All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

13. Files held on the school's network will be regularly checked by Mrs Maysey.

14. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
- Accessing another person's emails. All emails are double authenticated and it is not acceptable to ask to access someone else's emails.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting (See sections 8.0 in the WSCC ICT in schools Acceptable Use Protocol guidance).

- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data. (See section 9.0 respectively in the WSCC ICT in schools Acceptable Use Protocol guidance).
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from Mrs Maysey.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

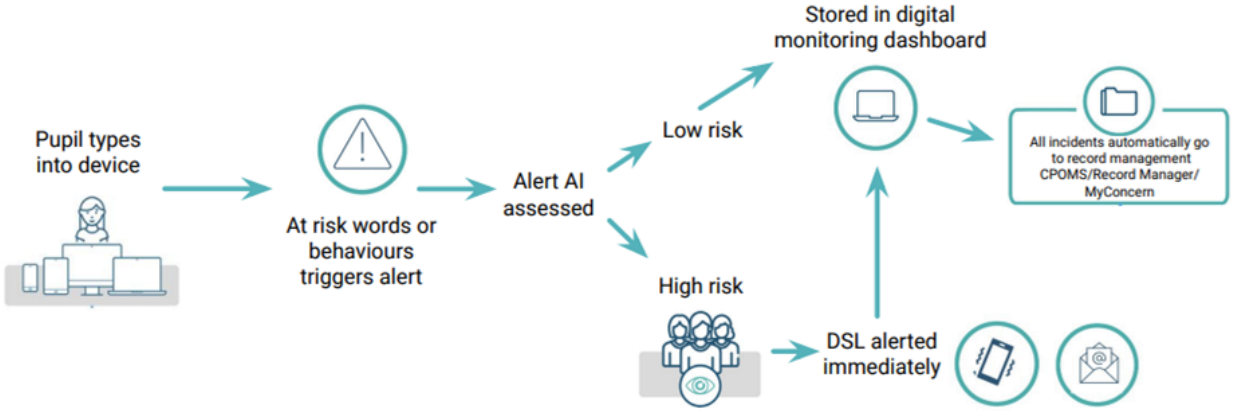
Users are expected to inform Mrs Maysey or Miss Webster immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network

FILTERING AND MONITORING

The school has robust filtering and monitoring systems to keep the children and adults safe when going online.

The filtering system, SurfProtect Quantum, is provided by Exa Networks through IT service provider JSPC. SurfProtect uses a range of technologies bolstered by human verification to accurately classify web content. The filtering for the children's logins differs from that of the teacher logins to allow an age appropriate filtering strength. All inappropriate content accessed in school, needs to be reported to Natasha Maysey who will report it to Exa Networks. This will ensure the content will subsequently be blocked by SurfProtect.

The monitoring system used at Aldingbourne school is Smoothwall. It is a managed monitoring system meaning that it is moderated by highly trained safeguarding professionals external to the school. If a person types a word, phrase or is behaving in a manner that is perceived as risky, an alert is triggered. It will then be vetted by AI who will assess whether it is low risk or high risk. If it is assessed as low risk the event will be stored, ready to be passed on to the record management at the end of the week. If it is assessed as high risk, it will be passed on to the monitoring team who will assess whether the DSL needs to be alerted immediately or whether it can be stored and passed on at the end of the week.



Examples of risk:
No Risk = Child Googling West Sussex
Low Risk = Child typing that they hate a friend
High Risk = Person looking at pornography or searching ways to self-harm.

The immediate contact for high risk events is Liz Webster (DSL & Headteacher). The deputy contacts (if Liz is unavailable) is Natasha Maysey (Assistant Headteacher & ICT coordinator), Sue Reed (Assistant Headteacher) and Ruth Tweed (DSD).

The system monitors the device at any location and regardless of whether the device is connected to the internet or not. This monitoring functions at a device level meaning that any user (staff, pupil or visitor) is kept safe.

AI

Our filtering and monitoring system is very limited to how it can work on AI content. Because of this, pupils do not have access to it. The filter cannot edit, modify or understand the AI model input nor respond directly. Smoothwall monitor will capture any keyboard input that is appropriate.
For the above reasons, all pupils and staff do not have access to generative AI. The exception to this is SLT and SENDCO, however this is only available on devices that are not used by pupils (the staffrooom).

MOBILE PHONES

Mobile phones are not permitted for use in the classroom or other teaching spaces within the school. The use of mobile phones by staff and visiting adults is limited to the staff room or offices. Children should not see staff using mobile phones as this is a modelled behaviour as all children MUST leave their phones in the office at the beginning of the day. The exception to this is when teaching emails, where a mobile phone will be required to double authenticate access to the teachers email account which is used to model how to send an email. If there is an emergency/medical reasons that you may be receiving a call during the working day, mobile phones must be left in the office.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of pupils are published.
Publishing includes, but is not limited to:

- the school website
- the Local Authority web site,
- web broadcasting,
- TV presentations,
- Newspapers.

Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.

To be reviewed by The Curriculum Committee every 2 years
Last Review 18.03.2026 (Full Governors)
Next Review October 2027