CALSHOT PRIMARY SCHOOL

Internet and E-Mail User Policy

'At Calshot we aim to provide the highest quality of learning and care for ALL children in a safe and enjoyable environment, nurturing personal values, in partnership with parents, carers and the wider community. We expect everyone in our school to strive to achieve their full potential.'

Internet and E-Mail User Policy

Networked resources, including Internet access, are 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 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 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. 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 the Head Teacher or Deputy Head Teacher.

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 password to anyone. If you think someone has learned your password then contact the Computing Lead to arrange a new password to be established.
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. Care should be taken over the content of e-mails. It is important that the inclusion of personal information and references should be avoided wherever possible. Where data is transmitted – use encryption through S2S secure DFE web address or Prospective the BCC secure web address.
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 the Computing Lead.
10. Do not introduce devices with removable storage into the network without having them checked for viruses.
11. Do not attempt to visit websites that might be considered inappropriate, such sites would include those relating to illegal activity. All sites visited leave evidence on the 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. Files held on the school's network will be regularly checked by the ICT technician.
13. 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 or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety.
- 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
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- 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.
- Using the Internet for personal financial gain.
- Using the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Using the internet to play games against an opponent.
- Use of chatrooms, other than those with a specific educational purpose.

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 the Computing Lead.
- All software should be properly licensed, registered and in accordance with the school's financial regulations.

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 the Head Teacher or Deputy head Teacher 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.
There should be no expectation of privacy in internet or e-mail usage by individuals. The school reserves the right to inspect any and all files stored in private areas of the network to ensure compliance with this policy.

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. Named images of pupils will only be published with the separate written consent of their parents or carers (included on the pupil registration form).

Publishing includes, but is not limited to:

- the school website
- the Local Authority web site,
- Newspapers.

SOCIAL NETWORKING

Social networking sites can leave professionals vulnerable due to the open nature of the Internet. Below are a set of guidelines which school policy require you to follow:

- Ensure that the privacy settings are set to 'Friends only'.
- Do not discuss any issues or personnel (i.e. staff, parents or pupils) relating to school.
- If you are named in an inappropriate reference /photo, you should contact the 'user' and ask for the content to be removed. If they refuse to remove the content, contact the social network provider and inform the head teacher.
- Ensure that you do not accept parents, pupils or past pupils as friends.
- Ensure that any comments/images that you put on the site could not be deemed as defamatory or in breach of copyright legislation.
- If you are the victim if cyberbullying, contact the social network provider and inform the Head Teacher.

If any issues arise relating to social networking, the school will not be in a position to support you; any support will have to be obtained from your professional body.

SAFEGUARDING

Pupils are made aware that if they receive any inappropriate images or messages via the internet, they need to report it to an appropriate adult immediately (ie parent or a member of the teaching staff).

INTERNET ACCESS AT HOME USING SCHOOL EQUIPMENT

- Staff should not use, or try to use, the internet for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts.
- Staff must be aware of, and abide by, the GDPR Code of Practice and act in accordance with the school's Data Protection Policy.
- Users should not do anything illegal.
- Users should not use the internet to intentionally access or transmit computer viruses or similar software.
- Only the member of staff to whom the computer has been loaned may use the computer to access the internet. Allowing other family members or friends to use school equipment to access the internet is strictly forbidden.
- Anti-virus software must be installed

Please see related policies:

- Data Protection Policy
- GDPR guidance
- Staff Code of Conduct
- Safeguarding Policy

This policy was reviewed by the Health, Safety and Welfare Committee on Thursday 17th June 2021