SHOREHAM ACADEMY

ACCEPTABLE USE POLICY

Reviewed Nov 2024

Next review Dec 2025

Introduction

The use of Information and Communications Technology at Shoreham Academy is about learning, especially e-learning. It is about improving children's life chances in education through the use of established and emergent technology to enhance learning outcomes. But it is also about those activities and experiences that enhance leadership and teamwork. In this sense, the Communications element of ICT sometimes takes precedence over the Information element. However, the use of ICT brings with it new concerns about attitudes and values. It is our task to ensure that these attitudes and values evolve to maximise students' opportunities to evolve into responsible citizens.

Adherence to the common mission of United Learning is one of the tests that must be applied to the use of ICT in our school. Clear goals are spelt out in our academy, a vision for ICT and its use is articulated as part of our digital strategy.

In the implementation of ICT to support e-learning, there is a commitment to raising standards. Although there is a great deal of technical information included in this publication it must never be forgotten that ICT in education is about learning and teaching. These guidelines are designed to help schools to put in place educational and technical policies that will make ICT live up to its promises.

Educational ICT Vision

Shoreham Academy has a curriculum that is designed to specifically reflect national and local aspirations, career and Higher Education opportunities and the skills and talents required in the community. ICT installed in our school reflects this curriculum, as well as providing technological tools to enhance high-quality teaching and learning. Every classroom has an interactive touchscreen connected to a computer allowing the preparation and delivery of dynamic, interactive lessons across all curriculum areas. Internet facilities are available in learning spaces and every teacher and student has an email address, a Firefly VLE account, access to Office 365 and access to materials that allows collaboration and home access to teaching and learning materials.

Both students and teachers have access to computer resources, e-learning material and a learning platform (Firefly VLE). The ICT is driven by sophisticated Local Area Networks (LAN) that ensure safe, secure and timely access to e-mail, e-learning resources, printing, the Internet and educational software.

Other facilities within our academy include computerised administration systems as well as specialised equipment used for specific subject areas. The curriculum is supported by the learning and teaching resources provided, which include up-to-date ICT facilities. High quality professional development ensures that teachers are amongst the best trained ICT practitioners in the country. A full programme of Touchscreen training is offered to all staff. ICT Technical staff and teaching staff who lead on technology in their department undertake additional training as part of our CPD programme which supports the delivery of teaching using the Rosenshine principles supported by technology. This training, along with ICT resourcing combines with exciting and innovative teaching practices to help

ensure that students enjoy the best learning experience possible, giving them the skills and the knowledge necessary for success in the 21st century.

It is the Principal's responsibility to satisfy themselves that policies are in place that adequately reflect the ethos and curriculum of the school as well as informing practice. It is the responsibility of every staff member, both teaching and non-teaching, to ensure that the spirit of the policies is implemented across all relevant areas of learning, teaching, administration and support.

The use of ICT within the school or academy to support learning, teaching and administration is not an optional extra to be avoided. Neither is it to be used indiscriminately. ICT should be used where appropriate to enhance the learning experience of students and to facilitate best teaching practice by teachers. Administrative systems must be used to improve effectiveness, achieve efficiencies and promote best practice. Line managers will have responsibility to ensure that ICT usage achieves all of the above.

Student E-mail and Internet Acceptable Use Policy

a) Students must read and sign the policy before they can be allowed to use school technology and the computer Systems, Internet or e-mail at school.
b) Students are responsible for using all technology in an appropriate manner.
c) Students are responsible for anything that is done from their account. They must not give their password or login name to anyone and should lock the screen if they leave their device.
d) Students must only access those services they have been given permission to use.
e) Students must not access the internet, school software or e-mail for inappropriate purposes.
f) Students must not attempt to gain access to websites that are restricted within the school.
g) The work/activity on the Internet, school software and e-mail must be directly related to their schoolwork.
h) Students must not damage or interfere with school equipment.
i) Students must not try to bypass school and ICT security settings.
j) Students must not try to access any data on school IT systems that they should not have access to.
k) Students must not interfere with other students' work or attempt to use their personal or school accounts.
l) Students must not give personal information to anyone on the internet or by e-mail.
m) Students must not download, use or upload, share via social media or send by email any material which is copyright.
n) Students must not view, upload or download or send by e-mail any material which is likely to be unsuitable for children, young people or schools. This applies to any material of a violent, dangerous, racist, or inappropriate sexual content. If they are not sure about this, or any materials, they must ask a teacher.
o) Students must be polite and appreciate that other users might have different views than their own. The use of strong language, abusive language or aggressive behaviour is not allowed.
p) Students must not write anything on a website, software platform or send by e-mail anything which could be offensive.

q) They must not use the internet, school software or social media in or out of school to bully, threaten or abuse other students or other members of the school community.
r) They must not use the internet in or out of school for any purpose that may bring the school into disrepute.
s) Students must use artificial intelligence (A.I.) technologies in an appropriate manner. If they are not sure about this, or any AI materials they are using, they must ask a teacher or member of SLT.
t) Students must agree to the school/academy viewing, with just reason and without notice any e-mails they send or receive, material they create, store or access on the school's computers, or logs of websites they have visited.
u) Students will comply with all aspects of other key ICT and Data protection policies including our Safeguarding & Child Protection Policy, E-Safety Policy, Image Use Policy and Behaviour policy.

Sanctions

Failure to comply with these rules will result in one or more of the following:

a) A ban, temporary or permanent, on the use of the Internet facilities at school.
b) A ban, temporary or permanent, on the use of the other ICT facilities at school.
c) A letter informing their parents of the nature and breach of rules.
d) Removal of use of school IT device, temporarily or permanently, if one is issued for home use.
e) Appropriate sanctions and restrictions placed on access to school facilities to be decided by SLT/ their Head of School/Head of Department. This could include pastoral/SLT detentions, internal exclusions or the Gateway reflection room, temporary suspension from school or in some circumstances permanent exclusion for serious abuse of the school's ICT facilities and of the internet.
f) In extreme cases or where behaviour is unlawful, the academy may involve the police.
g) Any other action decided by the Principal and Governors of the school.

If they do not understand any part of the Acceptable Use Policy, they must ask a teacher or member of staff.

Notes on Student E-mail and Acceptable Use Policy

Viruses, spyware and other forms of malware are common now and are usually introduced inadvertently. Schools and academies have effective, up-to-date software protection against viruses but students are also not permitted to undertake any online activity which may increase the risk of exposure to malware. Schools and academies have systems for dealing with deliberate misuse of computer systems, including the internet. Depending on the seriousness of the offence, internal sanctions might range from first warnings to temporary bans from using the ICT resources, to involvement of parents and guardians and in extreme cases permanent exclusion. Most offences are likely to be students experimenting and testing boundaries. However, if something more serious is suspected – for example, using the internet for illegal purposes, then it may be necessary to involve the police.

Monitoring

The use of the internet and e-mail raises issues when schools and academies wish to monitor their use by students. Essentially, a school or academy has a right and a statutory duty to monitor the use of the internet and e-mail systems to prevent it being used inappropriately, for unlawful purposes or to distribute offensive material. However, a student also has a right to fair treatment. It is the duty of schools and academies to balance these two separate rights. The first data protection principle states that data should be processed fairly and lawfully. Therefore, a school or academy should be open on the subject of monitoring and also conduct ICT lessons on the use of the Internet and e-mail and when individuals may use such systems for private communications. All e-mail is automatically scanned for unacceptable words, phrases and potentially dangerous links.

Schools and academies have the right to take all reasonable steps to prevent students from accessing inappropriate material on the internet or by e-mail. In the same way that students are taught the importance of keeping personal information private as part of their general awareness of internet and e-mail safety issues, they should also be familiar with the concept of data protection, both as a way of protecting information relating to themselves, and in terms of respecting information pertaining to others. As a general rule, children should be taught to always question why they are being asked for specific information on web sites or by e-mail, and seek guidance from a teacher or parent before providing any personal information.

What you do on academy computers is monitored and recorded by staff. This includes:

- Viewing your screen remotely
- Reading emails received and sent
- Logging internet sites accessed at the academy and on any academy devices used at home.
- Viewing files stored on the network
- Viewing files stored on Office 365 or Firefly
- Securus will record ICT misuse and potential safeguarding concerns for staff to view later.

Safety

Safe use of the internet and e-mail is important to both teachers and parents. Schools and academies providing student access to the internet, e-mail and other services must have systems in place to ensure that students use the technology safely, access only appropriate materials, and protect both themselves and school facilities from possible risks. The academy endorses the use of CEOP and other E-Safety materials to educate children and parents.

The academy needs to balance the desirability of fully exploiting the vast educational potential of internet and e-mail resources for learning and communication with safeguards against the risks and unacceptable activity. Our Acceptable Use Policy (AUP) will be signed by students and their parents, guardians or carers, as acceptance of the terms by which the school provides access and so forming a ‘contract’ for ICT use. Our acceptable usage policy is firmly embedded within the academy development plans and policies and will be signed by all students. This is not a ‘consent’ as provision of education requires all students to use ICT to fully access all elements of their education.

Implementation

Shoreham Academy has developed further policy documents that outline the basis for all aspects of acceptable use of ICT within the school or academy.

Related Policies

- Safeguarding & Child Protection Policy
- E-Safety Policy
- Image Use Policy
- Social Media Policy
- Behaviour Policy
- GDPR Data Protection Policies

It would obviously not be practical to ask students and parents to read and understand a full, detailed policy document, and so it is logical for schools and academies to develop a summary of the main acceptable use policy, setting out the ground rules for safe and responsible ICT use by students in institutions. Our AUP summary is written in a way that is appropriate for the age of our students, and is easily understandable. This AUP will be shared with students and parents before they start at the academy, and signed agreement gained that they will comply with it, so forming the basis of a contract between the academy, the student and parents.

A single page checklist will be posted next to all ICT facilities to remind students of the key elements of policies relating to the use of ICT. Our ICT policies are reviewed and updated at regular intervals.

Implementation

Clearly banning activity of any sort merely heightens the desire of young people to explore and push the boundaries. We have a responsibility to understand what children are doing by talking to them about their online activity and educating them to the possible downsides - encouraging safe use and enjoying the benefits whilst minimising the risks. Our academy will:

- Use CEOP and other ESafety materials to educate children about risks and benefits.
- Look at recommending software or social networking sites that safely enhance education experiences
- Provide timely and accurate information for parents and teachers.
- Provide safety tips and good advice.
- Stay up to date on developments.
- Include ESafety regularly within our PSHE curriculum

Legislation

The following are a list of Acts that apply to the use of the school computing facilities and which must be adhered to:

• Regulation of Investigatory Powers Act 2000.

• Computer Misuse Act 1990.

• Protection from Harassment Act 1997.

• Sex Discrimination Act 1975.

• Race Relations Act 1976.

• Disability Discrimination Act 1995.

• Obscene Publications Act 1959.

• Telecommunications Act 1984.

• Protection of Children Act 1978.

• Criminal Justice Act 1988.

• Data Protection Act 1998.

• The Patents Act 1977.

• Copyright, Designs and Patents Act 1988.

• Defamation Act 1996.

• Freedom of Information Act 2000.

• Human Rights Act 1998.

• General Data Protection Regulation 2018

• Online Safety Bill 2023

The academy should promote the highest standards in relation to good practice and security in the use of information technology. Consequently they should expect and support the integrity of their employees. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Data Security

Information held on the academy's computer systems may only be accessed with proper authorisation and if the information is pertinent to school work. Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computer Misuse Act 1990. It is policy to store data on a cloud drive where it is regularly backed up. The school will ensure that data that is not stored on the network online storage area is regularly backed up. Any mobile storage devices such as USB pen drives or external hard disks must be appropriately encrypted. Care should also be taken if the data network is used for the transmission or storage of CCTV images to

ensure that legal requirements are met. From September 2019 USB drives have not been permitted on any United Learning network and the only exception to use of USB devices is where it is an exam board regulation.

Copyright

Schools and academies must abide by copyright legislation if the intention is to use or publish materials through the internet. The use of online materials for teaching and learning is different from the use of printed and television or audio broadcast materials, which are covered by the Copyright Licensing Agency (CLA) and the Educational Recording Agency (ERA).

All materials published on the web (irrespective of format) are subject to copyright law and may not be copied or otherwise reproduced without the copyright owner's permission. Permission may be granted by the owner as stated at their site, or it may need to be obtained directly from the owner. It is insufficient just to acknowledge the source.

Just because something is published on the Web it does not automatically fall into the public domain. If Internet materials are clearly labeled as being copyright-free or in the public domain then it may be legally acceptable to use the materials.

Similar care should be used in copying music, video or other materials from CDs, CDROMs, DVDs or video streams. Possession of the originals does not automatically entitle the user to copy the contents in any format and may be illegal unless expressly authorized on the media or packaging itself.

Student E-mail and Internet Acceptable Use Policy Summary

- Students must read and sign the policy before they can be allowed to use school technology and the computer Systems, Internet or e-mail at school.
- Students are responsible for using all technology in an appropriate manner.
- Students are responsible for anything that is done from their account. They must not give their password or login name to anyone and should lock the screen if they leave their device.
- Students must only access those services they have been given permission to use.
- Students must not access the internet, school software or e-mail for inappropriate purposes.
- Students must not attempt to gain access to websites that are restricted within the school.
- The work/activity on the Internet, school software and e-mail must be directly related to their schoolwork.
- Students must not damage or interfere with school equipment.
- Students must not try to bypass school and ICT security settings.
- Students must not try to access any data on school IT systems that they should not have access to.
- Students must not interfere with other students' work or attempt to use their personal or school accounts.
- Students must not give personal information to anyone on the internet or by e-mail.
- Students must not download, use or upload, share via social media or send by email any material which is copyright.
- Students must not view, upload or download or send by e-mail any material which is likely to be unsuitable for children, young people or schools. This applies to any material of a violent, dangerous, racist, or inappropriate sexual content. If they are not sure about this, or any materials, they must ask a teacher.
- Students must be polite and appreciate that other users might have different views than their own. The use of strong language, abusive language or aggressive behaviour is not allowed.
- Students must not write anything on a website, software platform or send by e-mail anything which could be offensive.
- They must not use the internet, school software or social media in or out of school to bully, threaten or abuse other students or other members of the school community.
- They must not use the internet in or out of school for any purpose that may bring the school into disrepute.
- Students must use artificial intelligence (A.I.) technologies in an appropriate manner. If they are not sure about this, or any AI materials they are using, they must ask a teacher or member of SLT.
- Students must agree to the school/academy viewing, with just reason and without notice any e-mails they send or receive, material they create, store or access on the school's computers, or logs of websites they have visited.
- Students will comply with all aspects of other key ICT and Data protection policies including our Safeguarding & Child Protection Policy, E-Safety Policy, Image Use Policy and Behaviour policy.

Student E-mail and Internet Acceptable Use Personal Summary

- I will read and sign the policy before I use school technology and the computer Systems, Internet or e-mail at school.
- I am responsible for using all technology in an appropriate manner.
- I am responsible for anything that is done from my account. I must not give my password or login name to anyone and I will lock the screen if I leave my device.
- I will only access those services that I have been given permission to use.
- I will not access the internet, school software or e-mail for inappropriate purposes.
- I will not attempt to gain access to websites that are restricted within the school.
- My work/activity on the Internet, school software and e-mail will be directly related to my schoolwork.
- I will not damage or interfere with school equipment.
- I will not try to bypass school and ICT security settings.
- I will not try to access any data on school IT systems that I should not have access to.
- I will not interfere with other students' work or attempt to use their personal or school accounts.
- I will not give personal information to anyone on the internet or by e-mail.
- I will not download, use or upload, share via social media or send by email any material which is copyright.
- I will not view, upload or download or send by e-mail any material which is likely to be unsuitable for children, young people or schools. I understand this applies to any material of a violent, dangerous, racist nature and inappropriate sexual content. If I am not sure about this, or any materials, I will ask a teacher or member of staff.
- I will be polite and appreciate that other users might have different views than my own. I understand the use of strong language, abusive language or aggressive behaviour is not allowed.
- I will not write anything on a website, software platform or send by e-mail anything which could be offensive.
- I will not use the internet, school software or social media in or out of school to bully, threaten or abuse other students or other members of the school community.
- I will not use the internet in or out of school for any purpose that may bring the school into disrepute.
- I will use artificial intelligence (A.I.) technologies in an appropriate manner. If I am not sure about this, or any AI materials I am using, I will ask a teacher or member of SLT.
- I agree to the school/academy viewing, with just reason and without notice any e-mails I send or receive, material I create, store or access on the school's computers, or logs of websites I have visited.
- I will comply with all aspects of other key ICT and Data protection policies including our school's Safeguarding & Child Protection Policy, E-Safety Policy, Image Use Policy and Behaviour policy.