Shoreham Academy
The best in everyone™
Part of United Learning

Title	**ACCEPTABLE USE POLICY**
Policy Owner	**Tim Harkins**
Effective Date	**December 2025**
Last Revised	**December 2025**
Next Review Date	**December 2026**
Version Number	**5**
Target Audience	**Parents and students**

Contents

1. Introduction

At Shoreham Academy, technology is used to support learning and improve students' chances of success. ICT helps with lessons, teamwork, and communication, but it also brings responsibilities. We expect students to use technology safely and respectfully so they can become responsible citizens.

Our approach follows United Learning's mission and our school's digital strategy. ICT is not optional—it's part of teaching, learning, and administration. It should be used to improve education, not for inappropriate or careless purposes.

2. Educational ICT Vision

Shoreham Academy uses ICT to support its curriculum and improve teaching and learning. Every classroom has an interactive touchscreen and computer for creating engaging lessons. Students and teachers have access to email, Firefly VLE, Office 365, and online resources for collaboration and home learning.

Our ICT systems include secure networks for safe access to the internet, email, printing, and educational software. We also use specialised equipment for certain subjects and computerised systems for administration.

Teachers receive high-quality ICT training, and technical staff are trained to support teaching with technology. ICT is not optional—it should be used appropriately to enhance learning and teaching, and administrative systems should improve efficiency and best practice. The Principal ensures policies reflect the school's ethos and curriculum, and all student and staff must follow these policies.

3. Student E-mail, Internet and AI 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, AI tools 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, AI tools 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, AI tools 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, AI tools 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 (AI) technologies in an appropriate manner and in compliance with the section of this policy. 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.

4. 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, 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.

5. Notes on Student E-mail, Internet and AI Acceptable Use Policy

Viruses and other malware are common and often spread by accident. Our school uses up-to-date protection software, and students must not do anything online that could increase the risk of infection. If someone deliberately misuses ICT systems or the internet, the school will take action. Consequences depend on how serious the issue is and can include warnings, temporary loss of ICT access, contacting parents, or in extreme cases, permanent exclusion. Most problems are usually students experimenting, but serious cases such as undertaking illegal online activity may involve the police.

6. Monitoring

Schools have a legal duty to monitor internet and email use to prevent inappropriate, unlawful, or offensive activity. At the same time, students have a right to fair treatment. Shoreham Academy is open about the monitoring it undertakes and teaches students about safe and responsible use of email and the internet.

All emails are automatically scanned for harmful content and links. The school also take steps to block access to inappropriate material online. Students are taught to protect personal information and respect others' data.

They should always question why information is requested online and ask a teacher or parent before sharing personal details.

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.

7. Safety

Students must use the internet, email, and other online services safely, accessing only appropriate materials and protecting themselves and school systems from risks. The academy uses CEOP and other e-safety resources to educate students, staff and parents.

We aim to balance the benefits of online learning tools with safeguards against misuse. All students and their parents/carers must sign our Acceptable Use Policy (AUP), which sets the rules for ICT use. Signing the AUP is not optional, ICT is essential for accessing the full curriculum.

8. 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

Instead of asking students and parents to read a full policy, the academy provides a simple summary of the main rules for safe and responsible ICT use. This summary is age-appropriate, easy to understand, and shared before students start at the academy. Both students and parents/carers must sign it, forming an agreement with the school.

A one-page checklist of key rules will be displayed near all ICT facilities as a reminder. Policies are reviewed and updated regularly.

Rather than just banning activities, we talk to students about their online behaviour, explain risks, and teach them how to use technology safely while enjoying its benefits.

The academy will also;

- 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

9. Artificial Intelligence (AI) Acceptable Use

Students must use AI tools responsibly and in line with the school's educational objectives listed above. The following rules apply:

Purpose of Use
AI tools may only be used for school-related learning activities and tasks approved by teachers.AI must not be used to generate inappropriate, harmful, or misleading content.

Academic Integrity
Students must not use AI to cheat, plagiarise, or misrepresent work as their own. Any use of AI in assignments (even when used at home) must be declared, and students should follow teacher guidance on referencing AI-generated content. Where students use AI in exams, controlled assessments or coursework contrary to teacher instructions or those of exam invigilators then misuse would need to be reported to exam board and student's grades in that subject would be at risk.

Data Privacy
Students must not input personal information (their own or others') into AI systems. Students must not upload school data or confidential materials to external AI platforms.

Ethical Use
AI must not be used to create offensive, discriminatory, or harmful content. Students must not use AI for bullying, harassment, or spreading misinformation.

Verification and Critical Thinking
Students should verify AI-generated information and not assume it is accurate.AI outputs should be treated as a starting point, not a final answer.

Teacher Guidance
If unsure about appropriate AI use, students must ask a teacher or member of SLT before proceeding.

Monitoring and Sanctions
AI use will be monitored in line with school ICT policies. Misuse may result in sanctions, including loss of ICT privileges. Some AI systems and software will be restricted on the academy network.

10. 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

11. Data Security

Information held on the academy's computer systems may only be accessed with proper authorisation and if the information is pertinent to schoolwork. 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 must be appropriately encrypted. USB drives have not been permitted on any United Learning network since 2019 and the only exception to use of USB devices is where it is an exam board regulation.

12. 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.

Appendix 1 Student E-mail, Internet and AI 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.

Appendix 2 Student E-mail, Internet and AI 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, AI tools 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, AI tools 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, AI tools 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 (AI) technologies in an appropriate manner, if allowed to do so by my teachers. 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.