ACCEPTABLE ICT USE POLICY

Policy area

Parents, Students, Staff

Statutory regulation

N/A

SLT Lead

Director of Operations and Finance (Caroline Korniczky)

Last Updated

August 2024

Next review

August 2025

THE KING ALFRED SCHOOL ACCEPTABLE ICT USE POLICY

This policy should be read in conjunction with the following School policies:

- Anti-Bullying policy
- Data Protection Policy
- Data Retention Policy
- E-Safety Policy
- Safeguarding Children in Education Policy

1. INTRODUCTION

The purpose of this policy is to ensure that staff, students, parents and visitors understand the way in which the internet, email and computers should be used at the King Alfred School. The aim is to enable all staff and students including those children in the EYFS to gain maximum value from these facilities, to advise them of the dangers that can arise to themselves or the school if the technology is misused, and to advise staff and pupils of the consequences of misuse.

2. USE OF COMPUTERS IN SCHOOL

The provision of computers and associated technology is to support the education of students and to assist staff in the management of the school. To enable this:

- Priority in the use of computer rooms during lesson time will be for the conduct of timetabled lessons. If workstations are available during these periods, non-timetable students and staff may use the facilities with the permission of the teacher conducting the lesson.
- The school operates an "open policy" which means that students can use the computer rooms without staff supervision. This policy relies upon students exercising a high degree of personal responsibility. Computer rooms are at times open during break times and before and after school provided a member of the IT department has agreed to this.
- All computer equipment should be treated with care and staff and students should not attempt to alter the hardware or software configuration. If there is a need to make changes in line with day-to-day operations a member of the IT staff should be consulted.
- Any computers assigned to administrative purposes may not be used by students.
- No attempt should be made to disable or compromise the security of information contained within the school's computer network.

3. ONLINE BEHAVIOUR

As a member of the school community, you should follow these principles in all of your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without obtaining permission of the individual(s) concerned or the Director of Finance and Operations.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

4. USE OF THE INTERNET

Access to the internet is provided in the school as an educational, administrative and management tool. All users are expected to use the facility responsibly and with regard to the needs and wishes of others.

Unsuitable sites (for example, those containing offensive, obscene or indecent material) will be blocked where possible for students and staff. No attempt to bypass these restrictions should be made. If an unsuitable site is reached that is cause for concern then this should be reported to the IT staff, the Head, an Assistant Head or the Director of Finance and Operations. Students may be granted access to particular blocked sites when this is requested by a subject teacher. Similarly, staff may request the Director of IT to allow access to a blocked site. eSafe and Smoothwall technologies are amongst some of the monitoring systems used to protect students and staff online. Please also see Monitoring.

Access to the internet within school may not be used for personal financial gain, gambling, political purposes, advertising or any form of hacking, unless permission has been granted by the Head, the Director of Finance and Operations or the Director of IT

The use of web-hosted email accounts such as Hotmail and social media sites is allowed but these must be used responsibly and without giving offence to others and should not be used for school related business, particularly involving personal data.

Students are taught how to be safe online and what measures the school takes to help keep them safe in school, during IT lessons, Form Hour and PSHE lessons.

Pupils must not commit the school to any form of contract through the internet without the express permission of a teacher. Staff may only enter into a contract on behalf of the school through the internet in connection with the proper performance of their duties.

5. USE OF EMAIL

Staff and students may use school email for educational and school business and limited personal purposes, but they are expected to use it responsibly. This facility may be denied if a person uses it excessively for personal use, in a manner which could cause offence or distress to others, or in a way which compromises the day-to-day business of the school. The sending of offensive emails will not be tolerated (see Monitoring).

Users of the system should think carefully before sending or forwarding emails. If a student or member of staff receives an email clearly intended for another person they should inform the sender and redirect the email to the correct person. They must not use any information contained in the email nor tell anyone else about its contents, but they should immediately tell a member of the IT staff what has happened.

6. CONNECTION TO THE SCHOOL NETWORK

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Students and staff may only connect to the school network using their Sign-In Credentials. You should keep your password secret and not disclose it to anyone else. If you believe that your password has become compromised, either change it or seek the assistance of IT staff.
- You should only access school IT systems using your own username and password. Designated systems administrators may only use system passwords when carrying out their duties as administrators.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts.

7. PASSWORDS

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights

8. USE OF PERSONAL DEVICES OR ACCOUNTS AND WORKING REMOTELY

All school business must be conducted on school systems. When working remotely from personal devices you should access the school systems through VPN or Office365 and ensure no data is saved locally on your personal devices. The IT Team should be contacted to configure the VPN Link. Any school device used off-premise must be handed to the IT Team for encryption prior to removal from the school premises.

All staff should not use personal devices for any form of school communication, including the use of instant messaging services such as iMessage or WhatsApp. For Instant messaging, staff can make use of their school Teams account. In exceptional circumstances, staff may need to use WhatsApp on personal devices, for example when dealing with a safeguarding issue that requires immediate measures to resolve. However, where possible, this should take place on school provided phones using the schools WhatsApp business account rather than on personal devices.

Personal smartphones should not be used in the same room as students. Exceptions will be made for instances where a smartphone is necessary, for example when providing two factor authentication during the sign in process for school systems.

9. COMMUNICATION WITH PARENTS

All communication with parents must be conducted through school accounts and platforms. Staff may not communicate with parents on personal devices, unless there is an explicit reason for doing so, for example calling a parent regarding a sick child on a trip.

10. COPYRIGHT ISSUES

Generally, software purchased under licence cannot be given to students to install on personal computers. However, there are certain applications which we are allowed to share and students will be offered these where applicable.

Information obtained from internet sources will generally belong to a person or organisation and may have copyright restrictions. Such information, including text, graphics, sounds and moving images may not be published outside the school in any form. However, the law permits that **this information may be used in internal publications or, specifically, for examination coursework**. Where such information is used ownership must be acknowledged in a bibliography.

11. MONITORING

In the rare cases where the school has reason to believe that a student or member of staff has been misusing the school's computer network, Internet or email, we will investigate that person's use of these facilities. However, the school will normally respect the privacy of an email if it is clearly marked as personal, unless the school honestly believes that there are good reasons to examine its contents. Students and staff must be made aware that the school's software does screen for inappropriate usage and the school has the right to investigate and to follow up on any issues.

12. RETENTION OF DIGITAL DATA

Staff and pupils must be aware that the Data Retention Policy will apply to all emails sent or received through the school's systems. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders or inboxes. Hence it is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague.

All digital images of children must be stored on school cloud services and/or physical devices. Staff are not permitted to have digital images of students on their devices in the

context of them operating as a teacher. This does not include images of children that have been taken by a staff member when they are acting in the context of themselves being a parent. For example, photos of their child and students at a birthday party outside of school where the staff member attended as a parent, not a teacher.

All staff must be aware that they may not take images of children whose parents have not given permission for their child to be photographed. The list of children for whom permission has not been obtained can be provided from the school's Communication department.

13. BREACH REPORTING

The law requires the school to notify data breaches. If you have lost or think you might have lost any personal data or that an unauthorised person may have access to that data, you should contact the Director of Finance and Operations immediately. Personal data is any data that identifies an individual which for example may include email address, name or address.

14. BREACHES OF THIS POLICY

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Director of Finance and Operations. Reports will be treated in confidence.

A deliberate breach of this policy may be dealt with as a disciplinary matter using the school's usual procedures. Unauthorised access to or modification of computer material may leave perpetrators open to prosecution under the Computer Misuse Act 1990.