Acceptable Use

Date of Approval: 05 June 2025

Signed: Ruth Minhall

Position: CEO

Next review: 04 June 2026

Contents

Acceptable Use 1

Introduction and Aims 2

Relevant Legislation and Guidance 3

Definitions 3

Unacceptable Use 4

Staff (including governors, volunteers, and contractors) 5

Students 9

Parents 11

Data Security 12

Protection from Cyber Attacks 14

Internet Access 15

Monitoring and Review 16

Introduction and Aims

Information and Communications Technology (ICT) is an integral part of the way our Education Service works, and is a critical resource for students, staff (including the Senior Leadership Team), governors, volunteers, and visitors. It supports teaching and learning, pastoral, and administrative functions of the Education Service. However, the ICT resources and facilities our Education Service uses also pose risks to data protection, online safety, and safeguarding.
This policy aims to:

- Set guidelines and rules on the use of Education Service ICT resources for staff, students, parents, and governors.
- Establish clear expectations for the way all members of the Education Service community engage with each other online.
- Support the Education Service's policy on data protection, online safety and safeguarding in line with Kent County Councils (KCC) Online safety policy. It also takes into account the DFE statutory

guidance Keeping Children Safe in Education (KCSIE), and the Kent Safeguarding Children Multi-Agency Partnership agreements.
- Prevent disruption to the Education Service through the misuse, or attempted misuse, of ICT systems.
- Support the Education Service in teaching students safe and effective internet and ICT use.

This policy covers all users of our Education Service's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.
Breaches of this policy will be dealt with in line with the Education Service's Behaviour Policy, Staff Code of Conduct and Staff Disciplinary Policy and Procedure.

Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

"Users": anyone authorised by the Education Service to use the ICT facilities, including governors, staff, students, volunteers, contractors, and visitors.

"Personal use": any use or activity not directly related to the users' employment, study, or purpose. "Authorised personnel": employees authorised by the Education Service to perform systems administration and/or monitoring of the ICT facilities.
"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs. See Appendix 4 for a glossary of cyber security terminology.

Unacceptable Use

The following is considered unacceptable use of the Education Service's ICT facilities by any member of the Education Service community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).
Unacceptable use of the Education Service's ICT facilities includes:

- Using the Education Service's ICT facilities to breach intellectual property rights or copyright.
- Using the Education Service's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the Education Service's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery).
- Activity which defames or disparages the Education Service, or risks bringing the Education Service into disrepute.
- Sharing confidential information about the Education Service, its students, or other members of the Education Service community.
- Connecting any device to the Education Service's ICT network without approval from authorised personnel.
- Setting up any software, applications, or web services on the Education Service's network without approval by authorised

personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Education Service's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the Education Service.
- Using websites or mechanisms to bypass the Education Service's filtering mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way.

This is not an exhaustive list. The Education Service reserves the right to amend this list at any time. The CEO or members of SLT will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Education Service's ICT facilities.

Staff (including governors, volunteers, and contractors)

Access to Education Service ICT Facilities and Materials

The Education Service's IT manager manages access to the Education Service's ICT facilities and materials for Education Service staff and students. This includes, but is not limited to:

- Computers, tablets, mobile phones, and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Education Service's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact

the SLT. To access this information, you will need to submit your reason/rational for accessing this information via email to SLT for approval.

Use of Phones and Email

The Education Service provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the Education Service has provided. Staff must not share their personal email addresses with parents and students and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the IT manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the Education Service to conduct all work-related business.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Personal Use

Staff are permitted to occasionally use Education Service ICT facilities for personal use subject to certain conditions set out below. Personal use of

ICT facilities must not be overused or abused. The CEO may withdraw permission for it at any time or restrict access at their discretion.
Personal use is permitted provided that such use:

- Does not take place during teaching time or periods of work.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no students are present.
- Does not interfere with their jobs or prevent other staff or students from using the facilities for work or educational purposes.

Staff should be aware that use of the Education Service's ICT facilities for personal use may put personal communications within the scope of the Education Service's ICT monitoring activities (see section 5.6). Where breaches of this policy are found, disciplinary action may be taken.
Staff are not permitted to use their personal devices, such as mobile phones or tablets, for any form of recording or images of students. They must use registered work devices.

Staff should be aware that personal use of ICT (even when not using Education Service ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents could see them.

Personal Social Media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

Staff must ensure that nothing posted to any form of social media could bring the Educational Service into disrepute in any way.

Remote Access

We allow staff to access the Education Service's ICT facilities and materials remotely.

Our remote access is managed by the Educational Service's ICT support provider The access is through a cloud-based system using one drive and SharePoint.

If staff are using their own IT equipment to access these locations, then they must ensure that they are following the Data Protection policy. They must ensure that only the materials they use are pertinent to their role or required at that time.

If there is a concern over what has been downloaded the IT manager is able to monitor and report what has been downloaded and accessed by a staff member. This would be at the request and agreement of SLT.

Staff accessing the Education Service's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Education Service's ICT facilities outside the Education Service and take such precautions as the DSL and Data protection officer has stipulated.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

Education Service Social Media Accounts

The Education Service has official social media pages, managed by our Marketing department. Staff members who have not been authorised to manage, or post to, these accounts, must not access, or attempt to access these accounts.

The Education Service has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of Education Service Network and Use of ICT Facilities

The Education Service reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.

Regular meetings are held to ensure that:

- The filtering and monitoring provision is reviewed at least annually
- The filtering and monitoring block harmful and inappropriate content without unreasonably impacting teaching and learning.

The Education Service monitors ICT use in order to:

- Obtain information related to Education Service business.
- Investigate compliance with Education Service policies, procedures, and standards.
- Ensure effective Education Service and ICT operation.
- Conduct training or quality control exercises.

- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Engagement and Education of Staff

The IT and Online Acceptable Use policy will be discussed with staff as part of induction and will be reinforced and highlighted as part of safeguarding responsibilities.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential when using Education Service systems and devices.

All members of staff should be aware that their online conduct out of Education Service could have an impact on their role and reputation within Education Service. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Members of staff with a responsibility for managing filtering systems or monitor IT use will be supervised by the Senior Leadership Team and will have clear procedures for reporting issues or concerns.

The Education Service will highlight useful online tools which staff should use according to the age and ability of the students.

Students

Students must adhere to the rules regarding Acceptable Use of the Education Service's ICT Facilities and Internet detailed in Appendix 2.

- All students are advised to be cautious about the information given by others on sites. This is because other people may not be who they claim to be.
- Students are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, **Education Service** details, IM/email address and specific hobbies/interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Students are asked to report any incidents of online bullying to the Education Service.
- Students should not meet anyone that they have met through the internet, unless accompanied by a trusted adult.

Access to IT Laptops

Students should use laptops which have been supplied to them via the Education Service for all learning and working in the Education Service and should be used in line with the Education Service's Imagery use policy.

Search and Deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation July 2022, the Education Service has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under Education Service rules or legislation. Searches will be completed by a member of the safeguarding team, under the supervision of another member of the safeguarding or Senior Leadership Team.

The Education Service can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the Education Service's rules.
Staff members may also confiscate devices for evidence to hand to the Police, if a student discloses that they are being abused and that this abuse contains an online element.

Unacceptable Use of ICT and the Internet Outside of Education Service

Cases of unacceptable use of ICT and the internet by students when not on Education Service premises will be reviewed as required and sanctions will be applied in accordance with the Education Service's Behaviour policy.

Education

- Online safety will be promoted and embedded throughout the whole Education Service, to raise awareness regarding the importance of safe and responsible internet use amongst students.

- Education about safe and responsible use will precede internet access.
- Students will be supported in reading and understanding the IT and Online Acceptable Use policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.

- Online safety will be included in the PSHEE, RSE and other relevant programmes of study.

- Safe and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the Education Service's internal online safety education approaches.

- The Education Service will reward positive use of technology by students.

- The Education Service will implement peer education to develop online safety as appropriate to the needs of the students.

Engagement and Education of Children and Young People Considered to be Vulnerable

The Education Service is aware that some students may be considered to be more vulnerable online due to a range of factors.

The Education Service will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate (e.g., SENCo).

Parents

- Parents and carers are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Parents and carers are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, Education Service details, IM/email address and specific hobbies/interests).
- Parents and carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Parents and carers are asked to report any incidents of online bullying to the Education Service.

- The Education Service advises parents and carers to locate PC's and laptops in a highly visible part of the home, which can be regularly monitored.

Access to ICT Facilities and Materials

Parents do not have access to the Education Service's ICT facilities as a matter of course. However, parents working for, or with the Education Service in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access or be permitted to use the Education Service's facilities at the CEO's discretion. Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating With or About the Education Service Online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the Education Service through our website and social media channels.

Parents will be allowed to film and take images of their child during performances/sporting event, any image or video taken that includes other children outside of their family must not be shared online or on any social media account as other students may also be included in such material.

Data Security

The Education Service is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the Education Service cannot guarantee security. Staff, students, parents and others who use the Education Service's ICT facilities should use safe computing practices at all times.

Passwords

All users of the Education Service's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will use a password manager to help them store their passwords securely. The IT manager will generate passwords for students using a password manager/generator and keep these in a secure location in case students lose or forget their passwords.

When you first use this password, you will be asked to update with a password that you will be able to use and remember. It is expected that you will update this accordingly and keep this to yourself as these accesses your own private data and information. Passwords should contain a minimum of eight characters.

Software Updates, Firewalls and Anti-Virus Software

All the Education Service's ICT devices that support software updates, security updates and antivirus products will be configured to perform such updates regularly or automatically.
Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the Education Service's ICT facilities. Any personal devices using the Education Service's network must all be configured in this way.

Data Protection

All personal data must be processed and stored in line with data protection regulations and the Education Service's Data Protection policy. Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998 and GDPR. For more information on how the Education Service uses its data please refer to the Education Service's Data Protection policy.
Full information regarding the Education Service's approach to data protection and information governance can be found in the Education Service's Data Protection policy.

Access to Facilities and Materials

All users of the Education Service's ICT facilities will have clearly defined access rights to Education Service systems, files, and devices.
These access rights are managed by the IT manager.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Data manager and the IT manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Encryption

The Education Service ensures that its devices and systems have an appropriate level of encryption.

Education Service staff may only use personal devices (including computers and USB drives) to access Education Service data, work remotely, or take personal data (such as student information) out of Education Service if they have been specifically authorised to do so by the CEO.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the DSL.

Protection from Cyber Attacks

The Education Service will:

- Work with the IT provider to make sure cyber security is given the time and resources it needs to make the Education Service secure.
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Education Service's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email.
    - Respond to a request for bank details, personal information, or login details.
    - Verify requests for payments or changes to information.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:
    - 'Proportionate': the Education Service will verify this using a third-party audit annually, to objectively test that what security is in place is fit for purpose.
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe.
    - Up to date: with a system in place to monitor when the Education Service needs to update its software.
    - Regularly reviewed and tested: to make sure the systems are fit for purpose and secure as they can be.
- Back up critical data and this is completed once a day and store these backups on internal and external systems.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the Data protection manager.
- Make sure staff:
    - Enable multi-factor authentication where applicable.
    - Store passwords securely and do not share these with others.
- Make sure ICT staff conduct regular access reviews to make sure each user in the Education Service has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure.
- Develop, review and test an incident response plan with the IT provider, for example, including how the Education Service will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

Internet Access

The Education Service wireless internet connection is secure. In order to protect our students and staff, the Education Service employs the use of a filtering system to prevent access to unsuitable areas of the internet and monitors online activity.

We have separate levels of filtering and access for staff/students and visitors to the Education Service to ensure a secure environment and safe learning practices.

If students/staff or visitors come across any unsafe sites or practices, then they are to report this to the DSL.

Students

- Student access to Wi-Fi on Education Service issued devices is available.

- Student access to BYOD Wi-Fi is available.
- All Wi-Fi access is filtered and monitored via the Education Service's filtering and monitoring system.

- Students can request access to the BYOD through the DSL.
- Any concerns with online use will be monitored and actioned accordingly should there be belief of a

Staff

Wi-Fi access is filtered and monitored. Online activity is monitored. Any breaches will be investigated by the Senior Leadership Team.

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Parents and Visitors

Parents and visitors to the Education Service will not be permitted to use the Education Service's Wi-Fi unless specific authorisation is granted by the CEO.
The CEO will only grant authorisation if:

- Parents are working with the Education Service in an official capacity (e.g., as a volunteer).
- Visitors need to access the Education Service's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

Monitoring and Review

The CEO and SLT will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Education Service.