Cleves School
Learning Together

ICT and Internet Acceptable Use Policy

Reviewed on	January 2022 by Craig Smith
Guidance referred to	DfE Guidance 2019 published on The Key Surrey Guidance 2016
Reviewed by	Children's Achievement and Wellbeing Committee on behalf of The Board of Trustees of Cleves School
Review cycle	Every 2 years
Next review date	January 2024

1. Introduction and aims

ICT is an integral part of the way our academy works, and is a critical resource for pupils, staff, trustees, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the academy.

However, the ICT resources and facilities our academy uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, pupils, parents and trustees
- Establish clear expectations for the way all members of the community engage with each other online
- Support the academy's policy on data protection, online safety and safeguarding
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems
- Support the academy in teaching pupils safe and effective internet and ICT use

This policy covers all users of our academy's ICT facilities, including trustees, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the staff disciplinary policy.

2. 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 2018
- Searching, screening and confiscation: advice for schools

3. 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 academy to use the ICT facilities, including trustees, staff, pupils, 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 academy 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

4. Unacceptable use

The following is considered unacceptable use of the academy's ICT facilities by any member of the community. Any breach of this policy may result in disciplinary or behaviour proceedings

Unacceptable use of the academy's ICT facilities includes:

- Using the academy's ICT facilities to breach intellectual property rights or copyright
- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, its pupils, or other members of the community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy'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 academy'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 school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The academy reserves the right to amend this list at any time. The Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies. Copies of the staff code of conduct and staff disciplinary policy can be found on the Cleves Google Drive.

5. Staff (including trustees, volunteers, and contractors)

Access to school ICT facilities and materials

The academy's Senior Leadership Team manages access to the academy's ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets 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 academy'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 Deputy Headteacher or School Business Manager.

Use of email and phones

The academy provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the academy has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must no use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team. School devices are available for taking photographs both in school and on trips/sporting events.

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 which contains the personal information of another person, they must inform the Deputy Headteacher or School Business Manager immediately and follow our data breach procedure.

Personal social media accounts

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

Monitoring of school network and use of ICT facilities

The academy 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
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The academy monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective academy 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

6. Pupils

Unacceptable use of ICT and the internet outside of school

The academy will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on academy premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, other pupils, or other members of the community
- 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 academy's ICT facilities
- Causing intentional damage to ICT facilities or materials
- 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

7. Parents

Access to ICT facilities and materials

Parents do not have access to the academy's ICT facilities as a matter of course.

However, parents working for, or with, the academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the academy's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, 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 academy through our website and social media channels.

8. Data security

The academy takes steps to protect the security of its computing resources, data and user accounts. However, the academy cannot guarantee security. Staff, pupils, parents and others who use the academy's ICT facilities should use safe computing practices at all times.

Passwords

All users of the academy'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 pupils who disclose account or password information may face disciplinary action.

Software updates, firewalls, and anti-virus software

All of the academy's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. This will be managed by our IT support company

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 academy's ICT facilities.

Any personal devices using the academy'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 academy's data protection policy.

Access to facilities and materials

All users of the academy's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Deputy Headteacher and School Business 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 above 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.

9. Internet access

The academy wireless internet connection is secured and appropriate filtering is in place. Inappropriate searches or attempts to access inappropriate websites are logged and immediately flagged to the Senior Leadership Team. Filters are, however, not full proof and any inappropriate content should be immediately reported to the Senior Leadership Team.

Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Senior Leadership Team.

They will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's wifi 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)

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

10. Monitoring and review

The Senior Leadership Team monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

11. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection policy
- Code of Conduct
- Computing Policy

Appendix 1: Acceptable use agreement for pupils

Acceptable use of the academy’s ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school’s ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Use chat rooms
- Use a personal email address when emailing in school
- Email people I don’t know unless teacher has approved it.
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else’s name or password
- Give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.
- Look at other people’s files without their permission.
- Use school devices for online gaming, file sharing or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- Bully other people

I understand that the school will check emails and the websites I visit and how I use the school’s computers and equipment. This is so that they can help keep me safe and make sure I’m following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will use the school’s computers with care, ensuring I do not damage them through carelessness or inappropriate use. I will report all damages or faults to an adult immediately.

I will carry only one device at a time around the school, make sure it is put away carefully and plugged into the charging case correctly.

I understand that the school can remove my ICT privileges if I do certain unacceptable things online, even if I’m not in school when I do them.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: Acceptable use agreement for staff, trustees, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, trustees, volunteers and visitors

Name of staff member/trustee/volunteer/visitor:

When using the academy's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the academy's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Accept invitations from children or young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.
- Use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team
- Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network
- Share my password with others or log in to the academy's network using someone else's details
- Share confidential information about the academy, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the academy

I understand that all planning documents and associated materials, including those made personally, belong to the school. They must not be downloaded, used for financial gain, shared, or used elsewhere other than at Cleves School.

I understand that the academy can monitor the websites I visit and my use of the academy's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the academy's data protection policy.

I will ensure that I log off all apps and devices after my network session has finished.

I will let the designated safeguarding lead (DSL) and SLT know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/trustee/volunteer/visitor):	**Date:**