ICT and Internet Acceptable Use Policy

Fairfield High School

Approved by:	Board of Directors	July 2020
Signed by:	Chair of Directors	July 2020

Written by:	Owen Lloyd Assistant Head June 2020

Contents

1. Introduction and aims

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

However, the ICT resources and facilities our school uses also pose risks to GDPR, online safety and safeguarding.

This policy aims to:

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

This policy covers all users of our school's ICT facilities, including directors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our school behaviour policy, staff code of conduct and National Teachers' Standards.

2. Relevant legislation and guidance

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

- GDPR Act 2018
- The General GDPR 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 2020
- 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 school to use the ICT facilities, including directors, 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 school 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 school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school'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 school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school'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 school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programmes 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 school reserves the right to amend this list at any time. The Senior Leadership Team or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. This will usually only apply if there is a safeguarding issue.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policy.

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

5.1 Access to school ICT facilities and materials

The school's network provider (D&D) manages access to the school's ICT facilities and materials for school 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 school'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 their Line Manager who will raise the request with the Senior Leadership Team in the first instance and they will determine if additional permissions are needed and instruct D&D to authorise these changes if appropriate.

5.1.1 Use of phones and email

The school 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 school 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 GDPR 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 Senior Leadership Team 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 school to conduct all work-related business.

School phones should not be used for personal matters.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Senior Leadership Team 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 hours.
- 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 may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's ICT Policy.

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

Staff should take care to follow the school's guidelines on social media (see Appendix 1) and use of email (see Section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 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.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1).

5.3 Remote access

Staff accessing the school'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 school's ICT facilities outside the school and take such precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to GDPR legislation. Such information must be treated with extreme care and in accordance with our GDPR policy.

The school's GDPR policy can be found on the school website.

5.4 School social media accounts

The school has an official Facebook, Twitter and Instagram page, managed by SLT and Conor Giggle. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school 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.

5.5 Monitoring of school network and use of ICT facilities

The school 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 and at the request of or with the consent of the head teacher.

The school monitors ICT use in order to:

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

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to students only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff
- Students will be provided with an account linked to Google Classroom, which they can access from any device by signing in with their school Google Account.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school 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 school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the school behaviour policy if a student engages in any of the following **at any time** (even if they are not on school 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 school'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 school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, or other members of the school 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 school'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/Carers and Directors

7.1 Access to ICT facilities and materials

Parents/carers and directors do not have access to the school's ICT facilities as a matter of course.

However, parent/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) or Directors in school on official business may be granted an appropriate level of access, or be permitted to use the school's facilities at the head teacher's discretion.

Where parents/carers and directors 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 students, and help them learn, how to communicate respectfully with, and about, others online.

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

Accordingly, we ask parents and carers to sign the agreement in Appendix 2.

8. Data security

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

8.1 Passwords

All users of the school's ICT facilities are provided with a password which they will be required to change at first log in. All users should set strong passwords (a minimum of 6 characters, made up from a combination of letters and numbers) 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. Parent/carers, directors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the school’s ICT devices that support software updates, security updates, and anti-virus 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 implemented and maintained to protect personal data and the school’s ICT facilities.

Any personal devices using the school’s network must be configured in this way.

8.3 GDPR

All personal data must be processed and stored in line with GDPR and the school’s GDPR policy (see school website).

8.4 Access to facilities and materials

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

These access rights are managed by D&D.

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 Ms Lown who will notify SLT and D&D 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.

8.5 Encryption

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

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

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

9. Internet access and Wifi

The school wireless internet connection is secured.

The school will work with D&D to ensure that systems to protect students are reviewed and improved as required.

If staff or students discover unsuitable sites, the URL must be reported to SLT who will ask D&D to block the site.

If inappropriate sites have been deliberately accessed, the school will initiate disciplinary proceedings and/or sanctions as required. If the sites are potentially illegal or a part of a pattern of behaviour, the school will involve appropriate safeguarding, law enforcement and local authority professionals.

The school’s broadband access includes filtering appropriate to the age and maturity of students.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school monitors students’ use of the internet through software that flags up keywords that are used in search engines, websites and browsers. A screenshot is captured and recorded as evidence.

9.1 Parents/Carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's Wifi unless specific authorisation is granted by the head teacher.

The head teacher will only grant authorisation if:

- Parents/carers 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 head teacher and SLT 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 3 years and ratified by the Directors.

11. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- GDPR

Appendix 1: Staff and Social Media

Don’t accept friend requests from students on social media

Rules for school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your students
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your students online – once it’s out there, it’s out there forever.
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

---

Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, students and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- Conduct a **Google search for your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the head teacher about the request.

A parent or carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent, carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for Parents and Carers

Acceptable use of the internet: agreement for Parents and Carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page, Twitter, Instagram and MySchool App
- Email groups for parents (for school announcements and information)
- Our virtual learning platform (Google Classroom)

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues if they are not raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I am aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 3: Acceptable use of ICT agreement for Students

STUDENT ACCEPTABLE USE OF ICT AGREEMENT

Fairfield High School believes that new technologies have become integral to the lives of children and young people in today's society. The internet, other digital information and communication technologies are powerful tools, which open up new opportunities to everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

This agreement is intended to ensure:

- Students will be responsible users and stay safe while using the internet and other communication technologies for education, personal and recreational use.
- The school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Use of Equipment and other E-Technologies

- I am expected to treat ICT equipment carefully and not act in any way that might cause damage.
- I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I must report any faults or damage found to an ICT technician or teacher.
- Privately owned laptops and other devices must be registered with the Network Manager and I will follow the rules set out in this agreement, in the same way as if I was using school equipment whilst a personal device is being used in school.
- Mobile phones and camera phones will not be used in the classroom or around the school site, unless permission is given by the teacher.

Use of Email and Internet

- I understand that the school will monitor my use of the school ICT systems, email and other digital communications.
- I will not share my username and password nor will I try to use any other person's username and password.
- I will not search for, or display, any offensive or illegal material.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will not reveal personal details of myself or others in e-mail or any other form of electronic communication, or arrange to meet anyone without specific permission.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge.
- E-mail should only be used for work/educational purposes; it should not be used for personal e-mail.
- E-mails sent to an external organisation should be written carefully and authorised by a teacher before sending.
- I will be polite and responsible when communicating with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will not access social networking websites from the school network.

I am responsible for my actions, both in and out of school;

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and when they involve my membership of the school community (examples would be cyberbullying, use of images or personal information)
- I understand that if I fail to comply with this Acceptable Use Agreement, I may be subject to disciplinary action. This may include loss of access to the school network/internet and other appropriate school sanctions (in the event of illegal activities involvement of the police).

STUDENT ACCEPTABLE USE AGREEMENT

As a user of school ICT equipment I have read and agree to comply with the above Acceptable Use Agreement (AUP) when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDA's, Cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school emails, VLE, website, etc.
-

Student Name ……………………………………………………………….……………….

Signed ……………………………………………………………………………………….   Date………………...

Parent name …………………………………………   ……………………………………

Signed……………………………………………………………………………………..   Date…………………

Appendix 4: Acceptable use agreement for Staff, Directors, Volunteers and Visitors

Acceptable use of the school's ICT facilities and the internet:

agreement for Staff, Directors, Volunteers and Visitors

Name of staff member/director/volunteer/visitor:

When using the school'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 school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its students 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 school

I understand that the school will monitor the websites I visit and my use of the school'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 school's GDPR policy.

I will let the designated safeguarding lead and their deputies (DSL/DDSL) know if a student 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 school's ICT systems and internet responsibly, and ensure that students in my care do so too.

I have read and understand the ICT and Acceptable Use Policy

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