# ICT ACCEPTABLE USE



**Reviewed by:** Esther Palmer and Lara Hughes **Date:** September 2020

**Approved by Governors:** Richard Howard **Date:** September 2020

Introduction and Aims

ICT is an integral part of the way Frank Wise School works, and is a critical resource for pupils, staff, governors, 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 data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils and parents
- Outline the responsibilities of the school, Headteachers, technology subject leader, governors, staff, pupils and parents with regards to the use of ICT
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of technology systems
- Support the school in teaching pupils safe and effective internet and technology use

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

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 2020
- Searching, screening and confiscation: advice for schools

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 governors, 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 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

Acceptable Use

ICT is an invaluable tool for social, pastoral and administrative functions and at Frank Wise School we recognise the importance of using technology to enhance our children's learning.

Our aim is to teach children how to use technology safely and responsibly, rather than to simply avoid ever working with such tools. Responsible teaching and guidance will help pupils to understand what safe and responsible online behaviour means. This will not only safeguard from and reduce the risks of pupils coming into contact with strangers and other forms of unwanted sexual content and material, but also safeguard them against other forms of aggressive behaviour such as cyberbullying and commercial Internet issues such as financial scams through to receiving unwanted emails such as spam.

The Technology subject leader will act as eSafety co-ordinator and will be responsible for ensuring that the material used by all pupils and staff is suitable and appropriate for a school catering for pupils who have learning difficulties. It will also be the job of the eSafety co-ordinator to update and inform staff on new developments with regards to the safety of pupils. This may include attending a course such as the Child Exploitation and Online Protection (CEOP) training course then sharing the material that the qualified member of staff is allowed access to. The eSafety co-ordinator will also promote eSafety awareness across the school within the curriculum.

Staff responsibility also includes acting as a good role model to pupils by modelling good professional standards in their use of the internet through school provided equipment as well as their own.

*Frank Wise School provides internet access in order to :*

- Raise educational standards
- Increase opportunities for autonomous learning, practised safely
- Share and celebrate pupils achievements by showcasing their work using a variety of media such as photographs, video and audio
- Support curriculum development in all subjects
- Support the work of staff as its use is now an essential professional tool
- Enhance the school's management of information and administration systems
- Facilitate electronic communication and the exchange of data with the LA and others

*Frank Wise believes the educational benefits of using the internet to be :*

- Access to world-wide educational resources and information including museums, art galleries, research data, news and current events
- Information and cultural exchanges between students world-wide
- Increasing cultural, social and leisure activities in libraries, clubs and at home
- Enabling communication between staff & pupils, parents, carers & others in the community
- Technical support through forums and support sites
- It is an essential element of digital literacy

*Frank Wise believes that the internet can provide an effective medium for learning where :*

- Internet access is planned to enrich and extend learning activities as an integrated aspect of the curriculum
- Students are given clear objectives for internet use
- Students are provided with lists of relevant and suitable websites
- Students are educated to take responsibility for internet access and their own eSafety
- Students are made aware that the writer of an e-mail or the author of a web page may not be the person the claim to be and are taught to validate information before accepting it as true, or responding to it

- Students are taught to observe copyright when copying materials from the internet and to acknowledge their sources of information
- Access is reviewed to ensure it still meets curriculum needs

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that such material is inaccessible. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer or mobile device. It is essential that we teach pupils how to respond appropriately to unsuitable material, no matter how or when they encounter it. By teaching good practice within school we can support children in learning how to cope when outside the supervised context of the classroom. Please see also the Portable Technology policy and Online Safety policy.

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.

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 pupils, 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, 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

Social Network Sites

It is widely recognised that social media has many positive uses in a school environment, but as with almost every other method of communication, it is open to abuse.

Staff are expected to exercise the same moral standards in how they use social media as are expected in all other aspects of their professional role.

The school explicitly requests that staff only refer to their own work at the school in positive contexts in public, and this applies to the use of social media just as it does to casual conversations. Staff should not post anything on social media that damages the reputation of the school, regardless of whether in doing so staff identify themselves as a member of staff on their social media account. Neither should staff post photographs of pupils on their personal accounts, even if it is intended to celebrate them or the pupil's work. This can be done appropriately via the school website.

Staff should also make themselves familiar with the OCC document 'Simple Guidance for Staff in Education Settings on the Use of Social Network Sites' https://www2.oxfordshire.gov.uk/cms/sites/default/files/folders/documents/childreneducationandfamilies/workingwithchildren/networking.pdf for a broader overview of issues to do with posting or accessing media and considerations about suitability of making contact with pupils, ex-pupils and their families.

Responsibilities

*Of the School:*

- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken to protect pupils
- The Headteachers will ensure that the policy is implemented effectively
- Policy and procedures will be reviewed regularly
- All machines with internet capability accessed by pupils are sited in public areas
- The school will check that the sites selected for pupil use will be appropriate to the age and maturity of students
- The school will only use an internet service provider with capability to filter the material available to students or will take measures to ensure similar protection is installed on the school's computer system
- Any material that the school suspects is illegal will be referred to the LA

*Of the Technology Subject leader:*

- Will act as eSafety co-ordinator
- Will ensure that the material used by all pupils and staff is suitable and appropriate for a school catering for pupils who have learning difficulties
- To update and inform staff on new developments with regards to the safety of pupils
- Where appropriate, will attend training courses and share the materials. This may include things such as he Child Exploitation and Online Protection (CEOP) training course
- Will promote eSafety awareness across the school within the curriculum

*Of staff and pupils :*

- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the Headteachers or Technology lead who will inform the LA
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable
- Where appropriate, pupils and their parents will read this policy

*Of parents:*

- To inform the Headteachers if they become aware of or are worried about content their child is accessing and / or if they become aware of inappropriate online interactions, which may include the use of social media
- To model and help their child learn how to communicate respectfully with, and about, others online

The management of email in school

- Email is regarded as an essential means of communication and the school will take appropriate steps to monitor its use and content
- The language and content of emails should be of an appropriate level expected of any written work and should ensure that the good name of the school is maintained
- The forwarding of chain letters and anonymous letters is banned
- Staff and pupils should be aware that all email on the school system is regarded as public and as such will be monitored
- In most cases, pupils will only be given email access for educational activities through a group account e.g. as a class
- Where pupils are given individual email accounts these are only granted where a high level of trust can be assumed for its responsible use and in agreement with parents / carers
- Email messages on school business should be regarded as having been sent on headed notepaper
- Staff and pupils should be made aware of the potential for virus infection through the sending or opening of files attached to emails

Publishing material on the school's web site

- The school will maintain editorial responsibility for any school initiated website to ensure that content is accurate and quality of presentation is maintained
- The school will maintain the integrity of the school website by ensuring that responsibility for uploading material is always overseen by staff and that passwords are secure
- Pupils will be taught to publish for a wide range of audiences which might include governors, parents or younger children
- The point of contact on the website will be the school address, email and telephone number. Home information or individuals' email addresses will not be published

Publishing images and work of pupils

- The school recognises the sensitivity of families to photos, video clips, or the work of their child being widely distributed through printed, digital and online media
- As emphasised in the points above, the school believes that there are positive benefits for the children in collaborating with others and seeing themselves celebrated in the press and media
- However, we are also very conscious of the risks that children can be exposed to and whilst taking every care to teach them safe behaviours and to protect their interests, the decision on what materials can be published and to what extent lies with the family and the child
- There is a clear outline in Appendix 2 of categories of possible publishing of images and work of the pupils, with a helpful grid for parents and carers to notify us of what they deem to be acceptable

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, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

*Passwords*

- All users of the school'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. Parents or volunteers who disclose account or password information may have their access rights revoked

*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 we implement and maintain to protect personal data and the school's ICT facilities
- Any personal devices using the school'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 school's data protection policy

*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 sanctioned by the Headteachers and managed by the ICT service provider, which is currently ICON
- 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 Headteachers 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 school ensures that its devices and systems have an appropriate level of encryption
- School staff are provided with work devices and therefore the use of personal devices for accessing school data, working remotely, or taking personal data (such as pupil information) out of school is not permitted

<u>Visitors and volunteers</u>

Visitors to and volunteers of the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Headteachers.

The Headteachers may grant authorisation when:

- They are working in an official capacity
- They need to access the school's wifi in order to fulfil the purpose of their visit

<u>Monitoring and Review</u>

- The headteacher and subject leader for Technology will 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
- The governing board is responsible for approving this policy

This policy should be read in conjunction with:

- Online Safety Policy
- Portable Technology
- Safeguarding and Child Protection Policy

## Annex A: Useful contacts for further reference

| | |
|---|---|
| UK Council for Child Internet Safety (UKCCIS) | https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis |
| Child Exploitation & Online Protection Centre | www.ceop.gov.uk |
| Know IT all | www.childnet-int.org/kia |
| Think U Know | www.thinkuknow.co.uk |
| Childnet | http://www.childnet.com |
| Virtual Global Taskforce | www.virtualglobaltaskforce.com |
| Internet Safety Zone | www.internetsafetyzone.com |
| Internet Watch Foundation | www.iwf.org.uk |
| Childline | www.childline.org.uk |
| NSPCC | www.nspcc.org.uk |