The Firs Lower School

Acceptable Use and E Safety Policy

Contents and Quick links

Link	Page	Link	Page
1. Introduction	2	**12. E Safety**	6
2. Key Staff	2	**13. Safe use of images**	7
3. School ICT Equipment	3	**14. Storing data**	8
4. Portable ICT equipment	3	**15. Servers**	8
5. Mobile phones (and other portable devices)	3	**16. School Mobile Phones**	9
6. Monitoring	4	**17. Parental Involvement**	9
7. Breaches and Incident Recording	4	**Appendix 1 -** Pupil User Agreement	10
8. Passwords and password security	4	**Appendix 2 -** Adult User Agreement	12
9. Managing email	5	Appendix 3 - Use of SM Protocols	-
10. Internet Use	5	Firs GDPR Policy	-
11. Social Media	6	Location for Code of Conduct	-

1. Introduction

ICT is an essential resource to support learning and teaching, as well as playing an important role in our everyday lives. Consequently, we need to build in the use of these technologies in order to prepare our young people with the skills to access life-long learning and employment.

Whilst exciting and beneficial, both in and out of the context of education, all users need to be aware of the range of risks associated with its use

At The Firs Lower School*,* we understand the responsibility to educate our pupils on E Safety issues; teaching them the appropriate behaviours and critical thinking skills, to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people, to help them conduct their day-to-day activities. This data must be kept appropriately and safely in line with the school GDPR Policy.

In their use of ICT, staff must abide by The Firs Code of Conduct and any comments or posts via email or social media by staff (or stakeholders associated with The Firs Lower School) that are deemed to undermine the school values, can result in the same media or reputational damage. Any such incidents must be reported to the school SIRO, to be recorded as an E Safety incident and treated appropriately.

Everybody in the school has the shared responsibility; to represent the school values appropriately and to secure any sensitive information used in their day to day professional duties.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school such as PCs, laptops, tablets, chromebooks etc. and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones).

This Policy is designed to set out the rules, to manage the use of all ICT related equipment and online communication, in the best interests and to protect the safety of all children and other stakeholders at The Firs.

2. Key Staff

Position	Name
Head Teacher	Adam Campbell
Deputy Head	Kerry Mercer
Senior Information Risk Officer (SIRO)	Adam Campbell
ICT Administrator	Ellen Ashby

3. School ICT Equipment

a. As a user of the school ICT equipment, staff are responsible for their activity.
b. ICT equipment issued to staff will be logged with a record of serial numbers as part of the school's inventory.
c. All ICT equipment will be kept physically secure.
d. Staff will not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data.
e. Data will not be stored on PCs, laptops, or USB drives and **must** be stored safely in the Google Drives provided with staff email addresses.
f. A time locking screensaver will be applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
g. On termination of employment or transfer, all ICT equipment will be returned to the ICT administrator.
h. Staff are responsible to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive or confidential information is disclosed to any unauthorised person.
i. All ICT equipment allocated to staff must be authorised by the ICT administrator.
j. All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

4. Portable ICT equipment

a. Equipment must be kept secure to be covered for insurance purposes. When travelling by car, best practice is to place laptops in the boot before starting your journey.
b. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations or upgrades etc.
c. The installation of any applications must be authorised by the ICT administrator.
d. In areas where there are members of the general public, portable ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
e. Portable equipment must be transported in its protective case if supplied.

5. Mobile phones (and other portable devices)

a. The school allows staff to bring in personal mobile phones and devices for their own use. Under ***no*** circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
b. Staff are ***not permitted*** to use mobile phones when in the presence of children. They should only be used to send emails/texts or make calls etc. in the staff room or another room ***where children are not present***. (The only time this rule is superseded is in the advent of a 'lockdown' where, in line with the 'Lockdown Procedures,' email / text messages will be used to communicate with staff.)
c. Personal calls / texts should not be viewed or made during 'contact' time with children. Any urgent messages should be directed to the school office, who will be happy to bring you the message.
d. Staff must adhere to this policy when using their own device on school premises and when representing the school.
e. Pupils are not allowed to bring personal mobile devices/phones to school without a parent request form being completed and approved by school. (Y4 children who bring in a device, must leave it at the office and collect it at the end of the day).
f. The school is not responsible for the loss, damage or theft of any personal device.
g. The sending of text messages that could be deemed offensive, between any member of the school community, is not allowed.
h. No image or sound recordings are permitted to be recorded in school (or on a school visit) on these devices by any member of the school community.
i. Where the school provides mobile technologies such as laptops or tablet devices they must not be used to record personal data, including images and should not be used

privately outside as this might negate the school insurance cover.

6. Monitoring

a. The ICT administrator may inspect any ICT equipment owned or leased by the school at any time, without prior notice.
b. ICT authorised staff may monitor, intercept, access, inspect, record and disclose emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving staff or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the 'General Data Protection Regulation' (May 2018), or to prevent or detect crime.
c. The ICT administrator or headteacher may, without prior notice, access the school email account of someone who is absent, in order to deal with any school related issues retained on that account.
d. Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

7. Breaches and Incident Recording

a. A breach or suspected breach of policy by a member of staff, contractor or pupil, may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the individual concerned.
b. Any policy breach is grounds for disciplinary action in accordance with the school Code of conduct and Disciplinary Procedure.
c. Policy breaches may also lead to criminal or civil proceedings.
d. Any breaches or suspected breaches will be managed in accordance with the GDPR policy and/or Child Protection Policy as appropriate.
e. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO – The Headteacher.

8. Passwords and password security

a. Staff must always use their **own** personal passwords.
b. All temporary passwords must be changed at first logon.
c. Only disclose personal password to authorised staff.
d. Staff must never tell a child a password.
e. Staff must inform the ICT administrator or SIRO immediately If they are aware of a breach of security with a password or account.
f. Passwords must;
    - Contain a minimum of eight characters
    - Contain a mixture of upper and lowercase letters
    - Contain numbers and/or special characters
    - **Advice can be sought here: Password security - Google Support**
g. User ID and passwords for staff who leave will be deleted within ***48 hours*** by the ICT administrator or SIRO.
h. All users will read and sign the Acceptable Use Agreement, to demonstrate that they have understood the schools Acceptable Use and E Safety Policy.
i. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, including ensuring that passwords are not shared and are changed periodically.
j. Workstations must not be left unattended / unlocked. The automatic log-off time for the school network is ***15 minutes.***
k. The School Gmail accounts with accompanying access to Google Drives will have the

additional security of 'dual factor authentication' requiring the input of a password sent to a mobile phone or the selecting of 'yes' on the Google email app (to indicate it is the intended user) to log on.

9. Managing email

a. The school gives all staff their own Gmail account, to use for all school business as a work based tool.
b. The school email account should be the account that is used for all school business.
c. Staff sending emails to parents will add a cc. to the Headteacher (and any other appropriate member of the SLT) if, in their professional judgement, the communication could be significant, sensitive or urgent.
d. As stated in the staff Code of Conduct, any emails from parents/carers should be responded to within 36 hours during the working week.
e. Pupils will also be issued with a school Gmail account and this will be used under teacher supervision, for educational purposes.
f. Emails that need to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these emails will then correspond with the classes of records according to content in the school Information Audit document as part of the GDPR policy..
g. Emails created or received will be subject to disclosure in response to a subject access request under the GDPR. Staff must therefore actively manage their email account as follows:
    - Organise email into folders and carry out termly house-keeping on all folders and archives
    - Delete all emails of short-term value **at the end of every academic year**.
h. Staff ***must*** inform (the headteacher - SIRO) if they receive an offensive email. (The terms of the Staff Safety Policy also relate to email content)
i. *Staff **must never*** open attachments from an untrusted source; Consult the ICT administrator first.
j. Staff should not use the e-mail systems to store attachments. Detach and save business related work to the appropriate location on the individual staff member's Google Drive or in school shared drive.
k. Where an email must be used to transmit sensitive / confidential data, exercise caution when sending the e-mail and always follow these checks:
    - Verify the details, including accurate address, of any intended recipient
    - Do not copy or forward the email to any more recipients than is necessary
    - Request confirmation of safe receipt
    - In circular emails to parents, use blind carbon copy (Bcc), so email addresses are not disclosed to other recipients.
    - For very confidential material consider Encryption and password protection. See: Gmail encryption guide and send the information as an encrypted document.

10. Internet Use

Internet access:

a. The school provides pupils with supervised access to Internet resources and staff will preview any recommended sites before use (raw image searches are discouraged when working with pupils)
b. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
c. All users must observe copyright of materials from electronic resources
d. Staff will not post personal, sensitive, or confidential information or disseminate such information in any way that may compromise the intended restricted audience.
e. Staff will not reveal names of colleagues, pupils or any other confidential information

acquired through their job on any social networking site or online application.

f. As a representative of the school, staff will not post, re-post or send messages of an offensive nature or that undermine the core values of the school.

g. On-line gambling or gaming is not allowed within school premises or via IT equipment provided by the school.

Infrastructure and virus protection:

h. School internet access is controlled through a web filtering service.

i. Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

j. If staff or pupils discover an unsuitable site, the screen will be switched off / closed and the incident reported ***immediately*** to the SIRO.

k. It is the responsibility of the school, by delegation to the ICT administrator, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

l. Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT administrator.

m. If there are any issues related to viruses or anti-virus software, the ICT administrator, should be informed who will ensure that this is addressed.

n. Staff ***must not*** interfere with any anti-virus software installed on school ICT equipment.

11. Social Media

Facebook, Twitter, Instagram and other social media are increasingly part of our daily lives:

a. Staff ***are not*** permitted to access their personal social media accounts using school equipment ***when on the school premises.***

b. Staff are ***only*** permitted to access personal social media accounts on their own mobile phone or similar device, when they are in the ***staff room*** or another room where children are ***not*** present.

c. Pupils are not permitted to access any social media accounts whilst at school

d. Staff, governors and pupils are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

e. Staff understand that the school strongly advises that they should have tight security / privacy settings on any social media site used and that they must protect their professional identity online.

f. Staff are aware that if a parent makes contact on social media, to discuss a school matter, they must move this conversation off social media and suggest the parent contacts them or the school using the ordinary channels.

g. Staff and governors are aware as a representative of the school, they should not post, re-post or send messages of an offensive nature or that undermine the core values of the school.

h. Staff, governors, pupils, parents and carers are aware that their online behaviour and personal use of social media should at all times be compatible with the School Code of Conduct and UK law.

i. The use of social media by the school, to communicate with parents/carers and the wider community is governed by the Use of Social Media Protocols which are appendix 3 to this document.

12. E Safety

We believe it is essential for E Safety guidance to be given to the pupils on a regular and meaningful basis. E Safety is embedded within our curriculum and we continually look for new opportunities to promote it.

a. As part of the school Scheme of Work, there are agreed knowledge and skills objectives for teaching internet skills in Computing / PSHE and as part of the Firs' Theme Healthy Bodies, Healthy Minds.

b. Educating pupils about the online risks that they may encounter outside school is done informally, when opportunities arise and as part of the E Safety elements in the curriculum and special occasions, such as Safer Internet Day.
c. Pupils are taught about respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
d. Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also taught where to seek help if they experience problems when using the internet i.e. parent/carer, staff member, or an organisation such as Childline or the CEOP report abuse button.
e. Pupils are taught to avoid placing images of themselves on websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
f. Pupils are always reminded to avoid giving out personal details on websites, which may identify them or where they are e.g. name, address, phone numbers etc.
g. Pupils are advised they should not have social media profiles, although the need to set online profiles to maximum privacy and deny access to unknown individuals is covered (as it is recognized that many pupils will be using or will go on to use such sites.)
h. Pupils are asked to report any incidents of Cyberbullying to the school. (These will be recorded in the E Safety Incidents log and the Anti-Bullying log.)
i. ESafety information will be included in the newsletter, available on the school website and added in the messaging on school social media sites. Posters will be displayed & key advice promoted through displays etc.

13. Safe use of images

Digital cameras mean taking and publishing photos can be done in just a few simple clicks.

While the development of digital imaging has undoubtedly created massive benefits for learning, there are also some risks that your school needs to be aware of.

Use of images ICO Advice
NSPCC Photography & Sharing Images Guidance

Sharing and posting digital images to the internet, whether that be the school's website or social networking profile, mean that the pictures may well remain available online forever.

While you may want to celebrate class achievements or a child's work, there are issues which you need to be managed.

a. With written ('opt in') consent of parents / carers on the child's first admission to school, the school permits the appropriate taking of images by staff and pupils with school equipment.
b. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
c. Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
d. Staff (or pupils) are **not** permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images of pupils.
e. **Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.**
f. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. (A record of which pupils **do not** have this permission will be kept in a secure Google Document on the 'Pupil Information and Parent Meeting Drive'. This will be administered and updated as needed by the office team but will be accessible by all teachers so that they have up to date information regarding the acceptable use of pupils in images).

g. Social media posts and any linked images will be checked by the Social Media Team - see Use of Social Media Protocols - Appendix 3
h. Only the ICT Administrator, Headteacher or another member of the Social Media Team have authority to approve material and upload it to the web site or social media site.
i. In taking images staff should follow the following guidance:
   - Check that any child being photographed / filmed is on the list of parents/carers who have **not** given permission.
   - Any pictures should try to focus on group activities, rather than photos of an individual. Indeed, group photos should always be preferred over 'full face' pictures of individual children.
   - Try to take images showing the backs of children's heads or side views, again avoiding 'full face' images.
   - Names, especially full names, should not be used, and if they are, the names need to be kept separate from images.
   - When taking digital/video images ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

14. Storing data

Non image related data

a. Pupil and staff related data will be maintained safely on-line using the Integris G2 online database.
b. Some school financial data is held online in the financial database.
c. The remaining School financial information is held on a hard drive in the School Office. This will be migrated to the Google Drive as soon as possible.
d. All other school data will be stored safely on the school Google Drives provided as part of the Google School Domain.
e. The Google Drives will be protected by 2 factor authentication, requiring the input of a code sent to a staff member's phone, as well as the staff member's password.

Storage of Images

a. Images/ videos of children may be stored on the school's Google 'Media' Drive, where the images are held securely, protected by 2 factor authentication or on the password protected web site,
b. Pupils and staff are permitted to use personal portable media (e.g. tablets) for storage of images, although they should be downloaded to the Google Media Drive as soon as possible. (This should be done at least termly).
c. Rights of access to this material are restricted to the teaching staff and pupils.
d. ***Teachers*** have the responsibility of deleting the images on the Google Team 'Media Drive', when they are no longer required, generally after three years. (This is to allow photos to be used for promotional reasons). This is overseen by the ICT administrator, who may assist with this task of deletion of three year old files, each year.

15. Servers

a. Servers will be kept in a locked and secure environment
b. There will be appropriate limits to access rights
c. They will always be password protected
d. Existing servers will have security software installed appropriate to the machine's specification
e. Back up tapes will be encrypted by appropriate software
f. Data will be backed up regularly

g. Any back up discs will be securely stored off site.

16. School Mobile Phones

School mobile phones are generally reserved for occasional use e.g. on school trips and in emergencies if the main phone lines fail or are in constant use. They can be used to provide contact between staff on site however.

a. Staff are responsible for the security of the school mobile phone(s). Always set the PIN code on the school mobile phone and do not leave it unattended and on display (especially in vehicles).
b. Report the loss or theft of any school mobile phone equipment immediately.
c. The school remains responsible for all call costs until the phone is reported lost or stolen.
d. School mobile phones will only be used freely on site / in the presence of children if they are incapable of taking pictures.
e. School SIM cards must only be used in school provided mobile phones.
f. Never use a hand-held mobile phone whilst driving a vehicle.

17. Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting E Safety both in and outside of school and to be aware of their responsibilities.

a. Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
b. Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school E Safety policy through parent forums.
c. Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website / social media).
d. Parents/carers are expected to sign a Home School agreement containing the following statement or similar
   → **We will 'support the school approach to E safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community'.**
e. The school disseminates information to parents relating to E Safety where appropriate in the form of;

   - Information workshops
   - Posters
   - School website
   - Newsletter items
   - Social media posts

Appendix 1 -

Pupil Acceptable User Agreement
Safety Rules and E-Safety Rules

1. I will be responsible for my behaviour and/or actions when using any ICT equipment.
2. If I feel unsafe or worried when using any ICT, I will ask for help and tell my teacher or an adult in school, or someone I trust at home.
3. I will only use ICT in school for school purposes with the permission of a teacher.
4. I will support the school approach to e-safety and not deliberately upload or add any images, video, sounds or text that could upset any member of our school community.
5. I will not tell other adults or children my password.
6. I will only open/delete my own files with the permission of a teacher.
7. I will make sure that all ICT contact with other children and adults is responsible, polite, sensible and safe.
8. I will not deliberately look for, save or send anything that is nasty, unpleasant or rude.
9. If I accidently view something nasty, unpleasant or rude I will turn off the monitor and tell an adult straight away.
10. I will not give out my own details such as my home phone number, mobile phone number or home address in an e-mail or arrange to meet someone I don't know (unless it is part of a school project approved by my teacher and a responsible adult comes with me).
11. I will use my school allocated e-mail address in school and only use it to open my emails. I will use it at home sensibly and with permission from an adult.
12. I will only open any email attachments from people I know or someone my school has approved.
13. I will 'log off' at the end of a session on a computer or a mobile device
14. I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my E-safety.

Firs Lower School
E-Safety Pupil User Agreement

Dear Parent/Carer,

ICT, including the use of the internet, e-mail and mobile technologies, is a central part of our school and home lives. We aim to ensure that all children are safe and taught to be responsible when using any ICT.

The school accesses the internet through a filtering service provided by Central Bedfordshire County Council. Although this system is very effective at blocking sites providing unsuitable content, on rare occasions, some sites may slip through, at which point we will take immediate action to ensure the filtering service is notified.

We believe the benefits for pupils from accessing the internet exceed any disadvantage. Please note that children do not have access to any chat-rooms or other social networking sites at school. If the school ever has any concerns about your child's e-safety we will contact you and we would ask you to inform us if you have any concerns.

Please read (and if age appropriate) discuss the safety rules agreement attached with your child. As this 'User Agreement' plays a vital part in keeping our children safe, it is essential that you return this slip to school. In addition, we hope that you will support the school by promoting safe use of the internet and digital technology at home.

Thank you in advance for your support and cooperation, which is much appreciated.

Adam J G Campbell
Headteacher

✂--

E-Safety User Agreement

***Please tick appropriate box**

*I/We have read and will support the 'E-Safety User Agreement 'and will discuss this with my child when age appropriate □

*I/We have read and will support the 'E-Safety User Agreement 'and have discussed this with my child.□

Parent/Carer signature………………………………..

Name ……………………………………………………Class…………………………………

Appendix 2 -

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Ellen Ashby school ICT Administrator or Adam Campbell Senior Information Risk Owner (SIRO).

1. I will only use the school's email / Internet / Intranet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
2. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
3. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
4. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
5. I will only use the approved, secure e-mail system(s) for any school business.
6. I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
7. I will not install any hardware of software without permission of the ICT Administrator.
8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
9. Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
10. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
11. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher. I will respect copyright and intellectual property rights.
12. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
13. I will support and promote this policy and help pupils to be safe and responsible in their use of ICT and related technologies.
14. I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……..…………………….………… Date ……………………

Full Name ………………………………….......................................(printed)

Job title ……………………………………………………………………