St Faith's School Policies
Network and Internet Acceptable Use Policy

Related Policies

St Faith's adopts the following policies that relate to the Network and Internet Acceptable Use Policy:

- IT Security Policy
- Personal Device Policy for Staff and Visitors
- CCTV Policy
- School Privacy Notices
- Data Protection Policy
- Data Retention Policy
- Safeguarding Children Policy
- Staff Code of Conduct
- Taking, Storing and Using Images of Children Policy
- Data Breach Procedure
- Whistleblowing Policy
- Anti-Bullying Policy

Introduction.

The School intends that the Network and Internet are to be used as an enjoyable and educational resource, which will add to your knowledge base and can be used as a foundation for your further education and career.

There are however potential drawbacks with the use of the system, both for you and for the School.

The policy has been drawn up to protect all parties – the pupils, the staff and the School. Its purpose is to set out the principles, which you must bear in mind at all times and also give you some rules, which you must follow. As with every set of rules an occasion could arise which will fall outside them. In a case like this you should refer to the principles in this policy for guidance and if necessary refer the query to the IT Manager for clarification.

With the use of social networking becoming increasingly wide spread, it is important that this policy embraces the use of social networking sites. A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. It includes, but is not limited to, sites such as Facebook, Instagram, Snapchat, Twitter and Wikipedia.

A separate policy exists to inform and regulate the use of social media at St Faith's for both business and personal purposes, whether during School/working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or other IT equipment (including IT equipment belonging to staff). In any event, staff may not use their work email address for any personal use of social media.

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the School's IT Team.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's guidelines and procedures for the use of personal devices.

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education only. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts.

The contents of our IT resources and communications systems are the property of St Faith's. Therefore, staff and pupils should have no expectation of privacy in any email, file, data, document, facsimile, telephone conversation or social media post. There should also be no expectation of privacy in any other kind of information or communication transmitted to, received, printed from, stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, all activities using our IT resources and communications systems, including but not limited to social media postings and activities and internet sites visited. This allows us to ensure that our resources and communication systems are being used for legitimate business, safeguarding, conduct and performance purposes and to ensure that our network policy and principles are being complied with.

The School reserves the right to examine or delete any files that may be held on its computer files.

Staff and pupils should also be aware that all emails sent or received on school systems will be managed in accordance with the Data Retention Policy. Email accounts will be closed when a member of staff leaves the school and the contents archived] within 1 year of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the IT Manager.

Principles.

1. The facilities supplied by the School are for professional and educational purposes. They must only be used after you have received the appropriate training from a member of the Network Team, and only in accordance with the school's various policies including data protection.
2. Any property belonging to the School should treated with respect and care , and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the School's Network Team.
3. Portable data storage devices, such as external hard drives and USB memory sticks, must be used responsibly. Only school-provided, hardware encrypted USB drives may be used. These USB drives will be provided by the Network Team on request.
4. You must not bring the school into disrepute through your use of the network, e-mail, social media or the Internet.
5. During any timetabled lessons or other activities involving the children the use of e-mail and access to the Internet from the School's computers and network for Staff must be for educational use only. For Pupils the use of e-mail and access to the Internet from the School's computers and network must be for educational use only at all times
6. You must do all that you can to protect the security of the school's computer network, and the security of the networks belonging to others. This included participation in security related training.

(1) Passwords are updated in accordance with Government guidelines on an annual basis. All passwords shall be ten characters or longer and must contain at least one of the following: an uppercase letter, a special character and a number.
(2) Please do not use guessable passwords (i.e. family information) and passwords across accounts (i.e. Personal email account and work login account). Please do not write passwords down. The use of a Password Manager (i.e. KeePass) is strongly recommended.
(3) You should not divulge your network or any other application based passwords to anyone.
(4) If you believe any network or school application passwords have been compromised you must notify IT immediately so your password can be changed.
(5) You should be aware of the risks of computer viruses and take sensible precautions to avoid bringing them onto our system or passing them on to others.

7. You must not leave a computer that you are working on unlocked if leaving the device unattended for any period of time.
8. You must try to protect all personal and confidential information about yourself and others even if you receive or come across this information inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation.
9. You must not obtain (or attempt to obtain) access to any part of the computer system for which you do not have permission to enter or use. This is known as 'hacking' and is both a criminal offence and a serious breach of school rules.
10. You must not install any software or other active code on the School's systems without the permission of the IT Manager.
11. You should assume that, unless told otherwise, all material found on the Internet is protected by copyright.
12. Any messages or attachments sent over the network or the Internet must be appropriate and courteous, and must not contain anything which is pornographic, violent, racist, sexist, discriminatory, defamatory or blasphemous. To send such messages may be unlawful. As far as you are able, you must make sure that you do not search for or receive any such material. It is your responsibility to reject it if you come across it, and inform a member of staff.
13. You need to be aware of the risks posed by the online activity of extremist and terrorist groups. This forms part of the School's legal obligations in the respect of the 'Prevent' duty.
14. You must also read and abide by the contents of IT Security Policy and Personal Devices Policy for Staff and Visitors where applicable.

Breaches of this policy

Failure to follow the principles stated above, or the rules agreed to below, may lead to disciplinary action being taken. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy you should report it to the School's Data Compliance Officer (HR and Safeguarding Adviser / Judicium Consulting Ltd) or a member of the School's Breach Notification Team (please refer to the School's Breach Policy).

Richard Brent.

R P BRENT MBE
Bursar

Rules for members of Teaching Staff

1. I will only use the school's computer system whilst logged on with my own username and password.
2. I will never disclose my password to anyone.
3. I will not leave a classroom or common area without either logging off or locking any computers I have been using.
4. You'll need to register for MFA before accessing school data from outside of the school premises.
5. I will on finding any computer logged on and unattended either log it off or lock it.
6. All Internet activity whilst in a classroom or on any other activity involving children should be appropriate to staff professional activity. Internet activity at other times should be such that it does not bring the school into disrepute.
7. Before posting, I will consider whether a particular post puts my effectiveness as a teacher at risk. I will post only what I want the world to see.
8. I will report to my Head of Department or Line Manager immediately if I see any information on the Internet or on social networking sites that disparages or reflects poorly on the School.
9. I will immediately remove any Internet postings which are deemed by the School to constitute a breach of this or any other School Policy.
10. I will ensure that wherever possible privacy settings on social media sites are set so that pupils cannot access information relating to my personal life.
11. I will not use my personal email or social media accounts to contact pupils or parents.
12. Activity which threatens the integrity of the school Network system is forbidden.
13. I understand I am responsible for all e-mail sent and for any contacts made that may result in e-mails being received.
14. I will obtain prior written approval of the Headmaster for the wording of any personal profile which I intend to create where the School is named or mentioned on a social networking site.
15. I will seek approval from the Headmaster before I speak about or make any comments on behalf of the School on the Internet or through any social networking site.
16. I will not
    a. Provide references for other individuals on social or networking sites.
    b. Post or publish on the Internet or on any social networking site any reference to the School, my colleagues, parents or pupils.
    c. Use commentary deemed to be defamatory, obscene, proprietary or libellous. I will exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions and derogatory remarks or characterisations.
    d. Discuss pupils or colleagues or publicly criticise the School or staff in emails or on the internet such as on social media sites.
    e. Post images that include pupils.

f. Initiate friendships with pupils on any personal social network sites.

g. Accept pupils as friends on any such sites; I will decline any pupil-initiated friend requests.

h. Use social networking sites as part of the educational process, e.g. as a way of reminding pupils about essay titles and deadlines.

17. I will not read anyone else's e-mail without their consent.

18. I will not use the system for personal gain, gambling, political purposes or advertising.

19. I will respect the copyright of materials and not access or share material that infringes copyright. I will also not claim the work of others as my own.

20. I will not post anonymous messages nor will I forward chain letters.

21. I will apply the same professional levels of language and content in emails, social media posts etc. as for letters or other non-digital media.

22. I will not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, terrorism or extremism, or raises safeguarding issues).

23. I will ensure that pupils are not allowed access to the network without a level of suitable supervision.

24. I will ensure that when using the school network, pupils follow the network principles.

25. I will ensure that children are not accessing extremist or terrorist material when using the internet in school.

26. I will not load or allow a pupil to load any program or data from a CD or pen drive (USB stick) or other portable media storage device from outside school unless it has been checked by the IT Manager and they have given permission to do so.

27. I will not attempt to install software on, or otherwise alter, school IT systems.

28. I will not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and will not attempt to access parts of the system I do not have permission to access.

29. I will use only School-provided, hardware encrypted USB drives to hold School data.

30. I will treat the School computer equipment with care and report any faults or breakages.

31. I understand the school may monitor my use of IT resources and communications systems.

32. I will read and abide by any revisions to this agreement which may from time to time be issued by the Headmaster, the Bursar or the IT Manager. These will be circulated by email. The version of the agreement which appears on the share drive under Policies will be kept updated and I must consult this if I am doubtful about any aspect of the current policy.

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the IT Manager.

I understand and accept this Network and Internet Acceptable Use Policy.

Name: ___________________________________

Signed: ___________________________________

Date: ___________________________________

Rules for members of Support Staff

1. I will only use the school's computer system whilst logged on with my own username and password.
2. I will never disclose my password to anyone.
3. You'll need to register for MFA before accessing school data from outside of the school premises.
4. I will not leave a classroom or common area computer logged onto SIMS if I am not present in the room.
5. I will not leave a classroom or common area for more than a few minutes without either logging off or locking any computers I have been using. This includes locking any computers that might be in use at home for the purposes of school work and that are connected (via VPN or Remote Desktop) to the school network.
6. I will on finding any computer logged on and unattended either log it off or lock it.
7. All Internet activity during working hours should be appropriate to staff professional activity. Internet activity at other times should be such that it does not bring the school into disrepute.
8. When posting on social media I will post only what I want the world to see.
9. I will report to my Head of Department or Line Manager immediately if I see any information on the Internet or on social networking sites that disparages or reflects poorly on the School.
10. I will immediately remove any Internet postings which are deemed by the School to constitute a breach of this or any other School Policy.
11. Activity which threatens the integrity of the school Network system is forbidden.
12. I understand that I am responsible for all e-mails sent and that any contacts made that may result in e-mails being received.
13. I will obtain prior written approval of the Headmaster for the wording of any personal profile which I intend to create where the School is named or mentioned on a social networking site.
14. I will seek approval from the Headmaster before I speak about or make any comments on behalf of the School on the Internet or through any social networking site.
15. I will not:
    a. Provide references for other individuals on social or networking sites.
    b. Post or publish on the Internet or on any social networking site any reference to the School, my colleagues, parents or pupils.
    c. Use commentary deemed to be defamatory, obscene, proprietary or libellous. I will exercise caution with regards to exaggeration, colourful language, guesswork, obscenity. Copyrighted materials, legal conclusions and derogatory remarks or characterisations.
    d. Discuss pupils or colleagues or publicly criticise the School or staff – see comment above
    e. Post images that include pupils.
    f. Initiate friendships with pupils on any personal social network sites.
    g. Accept pupils as friends on any such sites; I will decline any pupil-initiated friend requests.

16. I will not read anyone else’s e-mail without their consent.

17. I will not use the system for personal gain, gambling, political purposes or advertising.

18. I will respect the copyright of materials.

19. I will not post anonymous messages nor will I forward chain letters.

20. I will apply the same professional levels of language and content as for letters or other media.

21. I will not use the network to access inappropriate material. This includes accessing sites promoting terrorist or extremist material.

22. I will ensure that pupils should not be allowed access to the network without a level of suitable supervision and that they are following the rules as laid down.

23. I will ensure that children are not accessing extremist or terrorist material when using the internet in school.

24. I will not load or allow a pupil to load any program or data from a CD or pen drive (USB stick) or other portable media storage device from outside school unless it has been checked by the IT Manager and they have given permission to do so.

25. I will use only School-provided, hardware encrypted USB drives to hold School data.

26. I will treat the computer equipment with care.

27. I understand the school may monitor my use of IT resources and communications systems.

28. I will read and abide by any revisions to this agreement which may from time to time be issued by the Headmaster, the Bursar or the IT Manager. These will be circulated by email. The version of the agreement which appears on the share drive under Policies will be kept updated and I must consult this if I am doubtful about any aspect of the current policy.

Signed:_________________________________ Print Name:__________________________________

Date:___________________________________

Rules for Year 5 to Year 8 Pupils

The school has installed computers and Internet access to help your learning. These rules are in place to help keep everyone safe.

1. I will only use the School's computer system whilst signed in with my own username and password.
2. I will never disclose my password to anyone.
3. I will only use the Internet in a way that is appropriate to my education.
4. I will not engage in any activity which threatens the safety of the School network.
5. I understand I am responsible for all e-mail sent and for any contacts made that may result in e-mails being received.
6. All Internet activity whilst in a classroom or when using online systems relating to the school should be appropriate.
7. I will not read anyone else's e-mail without their consent.
8. I will not use the system for personal gain, gambling, political purposes or advertising.
9. I will respect the copyright of materials.
10. I will not post anonymous messages nor will I forward chain letters.
11. I will apply the same professional levels of language and content as for letters or other media.
12. I will not use the network to access inappropriate materials. This includes accessing sites promoting terrorist or extremist material.
13. I will not bring any CD or pen drive (USB stick) or other portable media storage device from outside school unless I have been given permission to do so.
14. I will ask permission from a member of staff before using the Internet unless I have been instructed to use it as part of a lesson.
15. I will not give out any personal details, or arrange to meet someone, unless my parent, carer or teacher has given permission.
16. I will follow the procedure for signing in and out.
17. I understand that the School may check my computer files (including but not limited to Cloud Technologies) and may monitor my e-mail and the Internet sites I visit.
18. I will treat the School's computing equipment with care.
19. I will not use my personal email or social media accounts to contact members of St Faith's staff.
20. I will not initiate friendships with members of St Faith's staff on any personal social network sites.

Signed:________________________________ Print Name:_________________________________

Date:___________________________________

Rules for Year 3 and Year 4 Pupils

The school has installed computers and Internet access to help your learning. These rules are in place to help keep everyone safe.

1. I will only access the system with my own username and password, which I will keep secret.
2. I will not access other people's files.
3. I will only use the computers for school work and homework.
4. I will not bring in any CD or pen drive (USB stick) or other portable media storage device from outside school unless I have been given permission to do so.
5. I will ask permission from a member of staff before using the Internet.
6. All Internet activity whilst in a classroom or when using online systems relating to the school should be appropriate.
7. I will only e-mail people I know, or my teacher has approved.
8. The messages I send will be polite and responsive.
9. I will not give out any personal details, or arrange to meet someone, unless my parent, carer or teacher has given permission.
10. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and would help protect other pupils and myself.
11. I will follow the procedure for logging on and off.
12. I understand that the School may check my computer files (including but not limited to Cloud Technologies) and may monitor my e-mail and the Internet sites I visit.
13. I will treat the School's computing equipment with care.
14. I will not use my personal email or social media accounts to contact members of St Faith's staff.
15. I will not initiate friendships with members of St Faith's staff on any personal social network sites.

Signed:________________________________ Print Name:_________________________________

Date:__________________________________

Parents or Guardians Agreement

We ask that you as the parent/guardian of the child signing the above agreement read the agreement with your child and, if you are in agreement with your child having internet access under the above rules, and you are happy that your child understands the rules that he/she has agreed to, sign the form in the space below.

Signed:________________________________ Print Name:_________________________________

Date:__________________________________

Rules for Guest Network Users

1. I will only use the school's computer system whilst logged on with my own guest username and password.
2. I will never disclose my password to anyone.
3. I will not leave a classroom or common area without either logging off or locking any computers I have been using.
4. All Internet activity should be appropriate to staff professional activity.
5. Activity which threatens the integrity of the school Network system is forbidden.
6. Users are responsible for all e-mails sent and that contacts made that may result in e-mails being received.
7. I will not read anyone else's e-mail without their consent.
8. I will not use the system for personal gain, gambling, political purposes or advertising.
9. I will respect the copyright of materials.
10. I will not post anonymous messages nor will I forward chain letters.
11. I will apply the same professional levels of language and content as for letters or other media.
12. I will not use the network to access inappropriate material. This includes accessing sites promoting terrorist or extremist material.
13. External data or programs will not be able to be accessed unless authorised by the IT Manager.
14. I will treat the computer equipment with care.
15. I understand the school may monitor my use of IT resources and communications systems.

Signed:________________________________ Print Name:_________________________________

Date:__________________________________

Rules for Network Administrative Staff

1. I will normally use the school's computer system whilst logged on with my own username and password. For the purposes of Network Administration and problem solving I can log on using another username and password.
2. I will never disclose my password to anyone.
3. I will not leave a classroom or common area computer logged onto SIMS if I am not present in the room.
4. I will not leave a classroom or common area for more than a few minutes without either logging off or locking any computers I have been using.
5. I will on finding any computer logged on and unattended either log it off or lock it.
6. All Internet activity whilst in a classroom or on any other activity involving children should be appropriate to staff professional activity. Internet activity at other times should be such that it does not bring the school into disrepute.
7. I will post only what I want the world to see.
8. I will report to my Head of Department or Line Manager immediately if I see any information on the Internet or on social networking sites that disparages or reflects poorly on the School.
9. I will immediately remove any Internet postings which are deemed by the School to constitute a breach of this or any other School Policy.
10. I will ensure that wherever possible privacy settings on social media sites are set so that pupils cannot access information relating to staff personal lives.
11. Activity which deliberately or by negligence threatens the integrity of the school Network system is forbidden.
12. I understand I am responsible for all e-mails sent and that contacts made may result in e-mails being received.
13. I will obtain prior written approval of the Headmaster for the wording of any personal profile which I intend to create where the School is named or mentioned on a social networking site.
14. I will seek approval from the Headmaster before I speak about or make any comments on behalf of the School on the Internet or through any social networking site.
15. I will not
    a. Provide references for other individuals on social or networking sites.
    b. Post or publish on the Internet or on any social networking site any reference to the School, my colleagues, parents or pupils.
    c. Use commentary deemed to be defamatory, obscene, proprietary or libellous. I will exercise caution with regards to exaggeration, colourful language, guesswork, obscenity. Copyrighted materials, legal conclusions and derogatory remarks or characterisations.
    d. Discuss pupils or colleagues or publicly criticise the School or staff.
    e. Post images that include pupils.

f. Initiate friendships with pupils on any personal social network sites.

g. Accept pupils as friends on any such sites; I will decline any pupil-initiated friend requests.

16. I will not read anyone else's e-mail without their consent (or in specific cases the written approval of either the Headmaster or Bursar) other than mail caught by the Email filter where I shall read enough to enable me to decide as to whether it is legitimate or not. All Email read in this manner will be totally confidential.

17. I will not use the system for personal gain, gambling, political purposes or advertising.

18. I will respect the copyright of materials.

19. I will not post anonymous messages nor will I forward chain letters.

20. I will apply the same professional levels of language and content in emails, social media posts etc. as for letters or other non-digital media.

21. I will not use the network to access inappropriate material. This includes accessing sites promoting extremist or terrorist material.

22. I will take all reasonable steps to ensure that children are not accessing extremist or terrorist material when using the internet in school.

23. I will ensure that pupils are not allowed access to the network without a level of suitable supervision.

24. I will ensure that when using the school network, pupils follow the network rules.

25. I will not load or allow a pupil to load any program or data from a CD or pen drive (USB stick) or other portable media storage device from outside school unless it has been checked by the IT Manager and they have given permission to do so.

26. I will use only School-provided, hardware encrypted USB drives to hold School data.

27. I will treat the computer equipment with care.

28. I understand the school may monitor my use of IT resources and communications systems.

29. I will read and abide by any revisions to this agreement which may from time to time be issued by the Headmaster, the Bursar or the IT Manager. These will be circulated by email. The version of the agreement which appears on the share drive under Policies will be kept updated and I must consult this if I am doubtful about any aspect of the current policy.

Signed:_______________________________ Print Name:________________________________

Date:_________________________________

Rules for Pre Prep

The School would like the Network and Internet to be used to help you to learn well.

So that you can be safe you must follow the instructions given by grown-ups at home and teachers at school. At school you must follow these rules:

1. Only use the computers in the way that you have been shown by a teacher.
2. Only sign in to a computer if you have been given permission to by a teacher.
3. No email may be used unless a teacher says you can.
4. Keep your password secret.
5. Only use the Internet when a teacher tells you to.

Dear Parents

Please talk to your child about using the computer system at school according to the above rules.

Please sign below to agree that you are happy for your child to have internet access under the above rules.

Child Name: ______________________ Child Signature: ______________________

Parent Name: ______________________ Parent Signature: ______________________

Child’s Class: ______________________ Date: ______________________