Fairway Infant School
e-Safety Policy
February 2020

Adopted by the Full Governing Body
At their meeting on 4th February 2020
Review date February 2021

Aim of this Policy

At Fairway Infant School we recognise the impact that developments in technology have on education and society in general. We want to create a safe environment for all members of our school community (staff, pupils, volunteers and visitors), so that all users can make the most of the opportunities that the new technologies provide.

E-Safety is not just a technology issue, and responsibility for e-safety rests with all members of our community.

The school's e-safety policy will operate in conjunction with other policies including:

- Behaviour
- Anti-Bullying
- Safeguarding and Child Protection
- Data Protection and Security

E-Safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering.
- A member of staff being responsible for the implementation and monitoring of this e-safety policy.

Introduction

The purpose of this policy is to:

- Establish the ground rules for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our behaviour policy.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

Teaching and learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- School IT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.

School web site

- The contact details on the web site include the school address, e-mail and telephone number. Staff are named and can be contacted via the school office. Pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Pupils' full names are not used anywhere on the web site.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school web site.

Social networking and personal publishing

- The school blocks access to social networking sites.
- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school's broadband network is provided by EXA through our IT support company JSPC. Their filter only allows access to websites that have been cleared for use. All other websites are blocked.
- If staff or pupils discover an unsuitable site, it must be reported immediately to the Headteacher.
- Senior staff ensure that regular checks are made to ensure that the filtering methods are appropriate and effective.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones are not used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to GDPR May 2018

Policy decisions

Authorising Internet access

- All staff read and sign the 'Acceptable IT Use Agreement' before using any school IT resource.
- Pupil access to the Internet will be supervised access to specific, approved on-line materials.
- Parents are asked to sign and return a consent form.

Assessing risks

- The school takes all reasonable precautions to ensure that users access only appropriate material by using our broadband provider's filtering system.
- The school audits IT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the school's Safeguarding and Child Protection procedures.
- Pupils and parents are informed of the complaints procedure.

Communications

Introducing the e-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils are informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff have seen a copy of the school's e-Safety Policy and know its importance.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.

Enlisting parents' support

- Parents' attention is drawn to the school's e-Safety Policy in the school prospectus and on the school web site.

This policy will be reviewed annually by the governors and staff or in light of new guidance.

Adopted by the Full Governing Body
At their meeting on 4th February 2020
Review date February 2021

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

Sue Peckham
Chair of Governors

Appendix A - Acceptable Use Agreements

Staff Acceptable Use Agreement

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the Internet or the school's Intranet is not allowed. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users will accept personal responsibility for reporting any misuse of the network to the headteacher. Users are to take due care with the physical security of the hardware they are using.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.
Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the network manager.
9	I will ensure that I log off after my network session has finished.

10	If I find an unattended machine logged on under another uses username I will **not** continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the network manager.
15	I will not use “USB drives”, portable hard-drives, or personal laptops on the network without having them “approved” by the school and checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, eg a school parent and their children.
19	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
20	I will support and promote the school’s e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates the GDPR or breaching the security this act requires for personal data, including data held on the SIMS Learning Gateway.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and iPads are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the GDPR applies) that is sent over the Internet will be encrypted or otherwise secured.

Additional guidelines

- Staff must comply with the acceptable use policy of any other networks that they access.
- Staff will follow the "Safer Use Of The Internet By Staff Working With Young People" published within the West Sussex Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP
  A summary of this guidance is attached and forms part of this policy.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

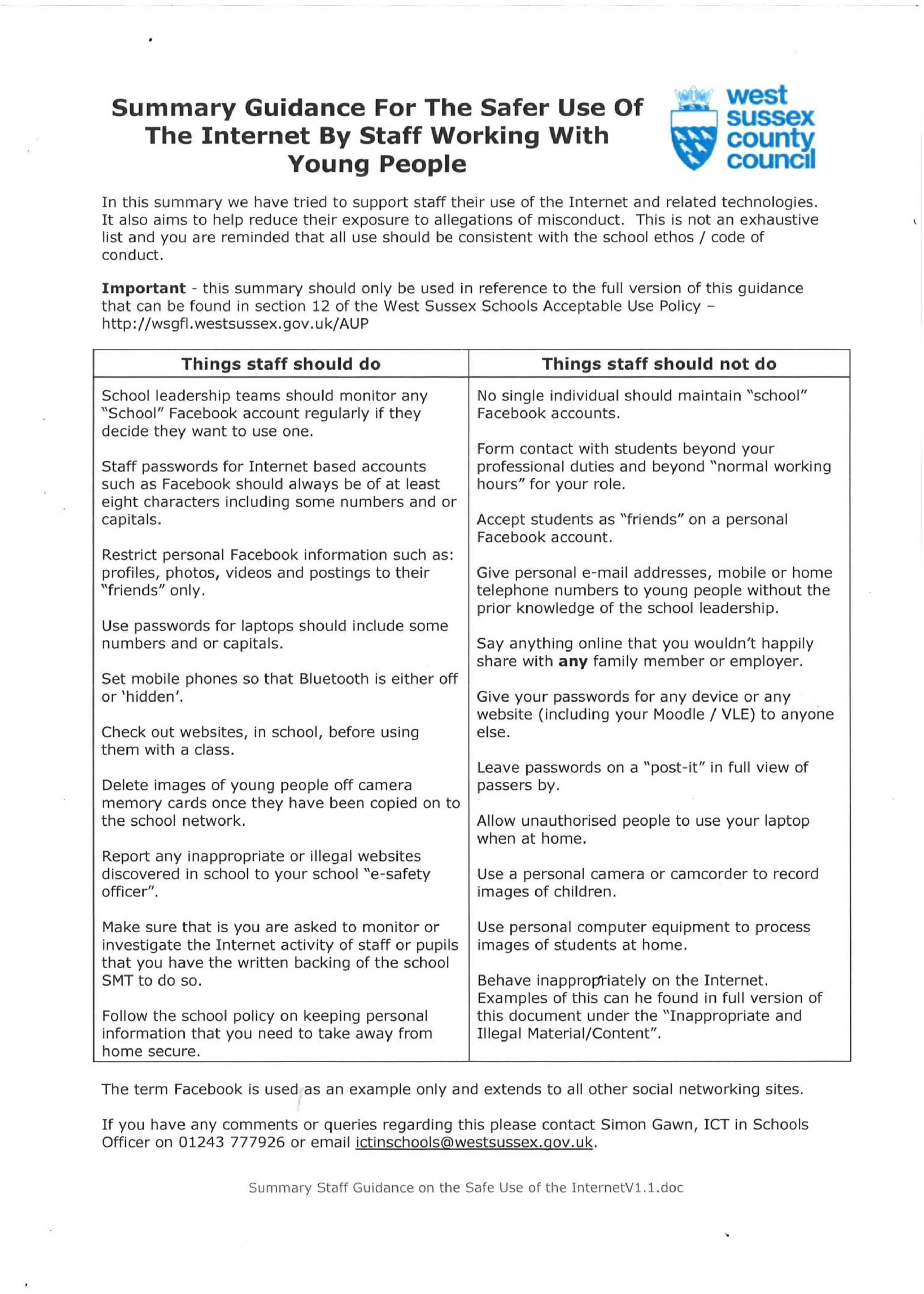
Users are expected to inform the network manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the network manager. Users identified as a security risk will be denied access to the network.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.



Summary Guidance For The Safer Use Of The Internet By Staff Working With Young People

west sussex county council

In this summary we have tried to support staff their use of the Internet and related technologies. It also aims to help reduce their exposure to allegations of misconduct. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos / code of conduct.

Important - this summary should only be used in reference to the full version of this guidance that can be found in section 12 of the West Sussex Schools Acceptable Use Policy – http://wsgfl.westsussex.gov.uk/AUP

Things staff should do	Things staff should not do
School leadership teams should monitor any "School" Facebook account regularly if they decide they want to use one. Staff passwords for Internet based accounts such as Facebook should always be of at least eight characters including some numbers and or capitals. Restrict personal Facebook information such as: profiles, photos, videos and postings to their "friends" only. Use passwords for laptops should include some numbers and or capitals. Set mobile phones so that Bluetooth is either off or 'hidden'. Check out websites, in school, before using them with a class. Delete images of young people off camera memory cards once they have been copied on to the school network. Report any inappropriate or illegal websites discovered in school to your school "e-safety officer". Make sure that is you are asked to monitor or investigate the Internet activity of staff or pupils that you have the written backing of the school SMT to do so. Follow the school policy on keeping personal information that you need to take away from home secure.	No single individual should maintain "school" Facebook accounts. Form contact with students beyond your professional duties and beyond "normal working hours" for your role. Accept students as "friends" on a personal Facebook account. Give personal e-mail addresses, mobile or home telephone numbers to young people without the prior knowledge of the school leadership. Say anything online that you wouldn't happily share with **any** family member or employer. Give your passwords for any device or any website (including your Moodle / VLE) to anyone else. Leave passwords on a "post-it" in full view of passers by. Allow unauthorised people to use your laptop when at home. Use a personal camera or camcorder to record images of children. Use personal computer equipment to process images of students at home. Behave inappropriately on the Internet. Examples of this can he found in full version of this document under the "Inappropriate and Illegal Material/Content".

The term Facebook is used as an example only and extends to all other social networking sites.

If you have any comments or queries regarding this please contact Simon Gawn, ICT in Schools Officer on 01243 777926 or email ictinschools@westsussex.gov.uk.

Summary Staff Guidance on the Safe Use of the InternetV1.1.doc

Fairway Infant School

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the network manager.
I agree to report any misuse of the network to the network manager.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the network manager.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the network manager.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: ____

Staff Signature : _______________________________

Date: _ _ /_ _ /_ _ _ _

Pupil Acceptable Use Agreement

WEST SUSSEX COUNTY COUNCIL
FAIRWAY INFANT SCHOOL
FAIRWAY, COPTHORNE, CRAWLEY, WEST SUSSEX RH10 3QD
Headteacher: Mrs B Davison Telephone: 01342 713691
Fax: 01342 718514
e-mail:office@fairway.w-sussex.sch.uk

January 2020

Dear Parents / Carers,

As part of the school's IT programme, we offer pupils access to the Internet. Pupils will only be allowed to use the Internet when supervised by a responsible adult. Our broadband filtering restricts sites available to pupils in the classroom.

Before being allowed to use the Internet, we require all pupils to agree to follow the enclosed school rules for the Internet and to obtain parental permission. Access will only be given if both you and your child sign and return the form below as evidence of your approval and their acceptance of the school rules on this matter.

A full copy of the school's e-safety policy is available on request.

……………………………………………………………………………………………

USER AGREEMENT & PARENTAL PERMISSION FORM FOR INTERNET ACCESS & MEDIA / ELECTRONIC RELEASE FORM

I have read and understood the school's rules for using the Internet and agree to keep them.

Child's name: ____

Child's signature: ____

Date: _____/_____/_____

As the parent / legal guardian of the pupil named above, I give permission for my child to access networked computer services such as electronic mail and the Internet. I understand that a responsible adult will always supervise pupils when using the Internet systems at school. I support the school's Acceptable Use Policy and will encourage my child to follow the guidelines.

Parent / Guardian's name: ______________________________________

Parent / Guardian's signature: ___________________________________

Date: _____/_____/_____

How to Use the Internet

These rules will help to keep me safe on the Internet

I will only use Internet sites agreed with my teacher.

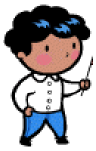
I must keep to the task I have been given.

I must not move to a different site without asking my teacher.

I must not write anything that might upset someone or give the school a bad name.

I must not tell anyone my full name, address or telephone number.

If I find something that I am not happy with, I will tell my teacher.



I know that my teacher will regularly check what I have on the school computers.

I must log off after I have finished with the computer.