INTERNET / E-SAFETY & ACCEPTABLE USE POLICY

Adapted from the WSCC model policy
Approved: 14 June 2023
Next review: June 2024

The Information Technology (IT) Coordinator is Paul Brown. Contact pbrown@rake.w-sussex.sch.uk

Introduction

1. At the DVSF schools, we recognise that information and communication technology plays an important part in learning. All learners in school must use technology appropriately, safely and legally. We have a responsibility to make all learners aware of the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. This policy is linked to, and works alongside, the DVSF schools' computing, child protection (safeguarding) and anti-bullying policies.
2. Our e-safety & acceptable use policy is based on West Sussex e-safety policy and government guidance. It has been agreed by the senior leadership team (SLT) and approved by the Interim Executive Board (IEB).
3. MS365 accounts are created for all staff and pupils. A remote working policy and codes of conduct for staff and pupils are in place. Parents are asked to sign consent forms for pupils for the relevant policy and code of conduct to be activated. Responsibility for e-safety and appropriate use of IT is managed by the IT Coordinator.
4. The Governing Body has responsibility for ensuring that the schools have an e-safety & acceptable use policy for IT and that this policy is reviewed annually.
5. The Executive Headteacher will ensure that there is a designated member of the senior leadership team for coordinating e-safety and acceptable use of IT, who will work closely with the designated staff responsible for child protection.
6. All staff have a responsibility to use IT appropriately and legally and report any illegal or inappropriate use of IT to the SLT or designated person for e-safety, as soon as possible.
7. Teachers and teaching assistants should address issues of e-safety when using the internet with children.
8. All children must follow all of the rules of the user agreement and network etiquette.
9. The IT Coordinator will ensure that computers have up-to-date virus protection and that the internet connection is filtered effectively with the support of e-safety and filtering specialists.

Use of the internet

10. The internet is an essential element of education, business and social interaction. Our schools have a duty to provide pupils 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.
11. Our schools encourage users to make effective use of the internet. Such use should always be lawful and appropriate. Internet usage means any connection to the internet, external e-mail or news groups.
12. Our schools expect all users to use the internet responsibly and strictly according to the following conditions: Users shall not visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:
    a. Pornography (including child pornography)
    b. Promoting discrimination of any kind
    c. Promoting racial or religious hatred
    d. Promoting illegal acts
    e. Any other information which may be offensive to colleagues
13. Incidents which appear to involve deliberate access to web sites, news groups and online groups that contain the following material will be reported to the police:
    a. Images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
    b. Adult material that potentially breaches the Obscene Publications Act in the UK
    c. Criminally racist material in the UK.
    d. If inappropriate material is accessed accidentally, users should immediately report this to the headteacher or designated e-safety coordinator so appropriate action can be taken.

System monitoring and filtering

14. Our broadband is provided through specialist internet service companies and all web filtering meets government and BECTA standards. All internet access provided to staff and children is filtered through the local authority's red filter, which automatically prohibits access to sites labelled in the categories described in the West Sussex Schools internet filtering policy (version 9.8). All staff and children are aware of the filtering system.

15. We have monitoring capabilities in school based upon the use of individual log-ins. A copy of all staff and pupil usernames and passwords are kept locked in the school safe and the headteacher can access these at any time.

Data protection and system security

16. All users on the system are expected to protect their own log-in details as a matter of personal and system security. **Under no circumstances should people allow other users to have their details or use their log-in**. If at any time a user feels that their password has been seen by another user they should log on and change their password immediately. It is also recommended that all passwords are alpha numeric.

User personal and system security code of conduct:

17. **Members of staff should never allow children to log on using staff (or other pupil) details**.

18. The e-safety coordinator will monitor inappropriate use on the system. It recognises users by their user name. By allowing others to use your details you will put yourself at risk of being wrongly accused of their impropriety. It will also negate the monitoring integrity as we will not be able to guarantee that user was responsible for the inappropriate use unless we can guarantee everyone is using their log-in details only.

19. User log-on details should not be shared under any circumstances. If a student does not have a log-in, report it to the IT Coordinator for them to resolve immediately.

20. When entering personal details on a web site log-in or the platform, users will often be asked if they *would like to save your details*. They should only save their details if it is their own personal computer.

21. The system does contain secure student details and staff documentation. If user details are seen by another person this data could be compromised and the password should be changed immediately.

22. If accessing school data from home on personal or school-provided hardware, users should always ensure, by following the aforementioned code, that data integrity is respected at all times. Equipment is more vulnerable once it leaves the building. Laptops, mobile technology and USB drives are susceptible to theft and loss along with data.

Digital media

23. Digital media and photographs play an important part of recording events in school life. We provide still and video digital cameras for use by children and staff. Staff should not use their own computers or mobile phones to record images. Non-staff adults helping in school or on school trips, must not use personal cameras or other devices to take pictures (including of their own child/ren.) Staff should make outside helpers aware of the *Volunteering in school* leaflet. Images of children may only be stored on the school's computers.

Staff e-mail

24. Any communication with children via e-mail should be through the staff school e-mail account only. Personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) should never be made available over the internet.

- Pupils may only use approved e-mail accounts on school systems.
- Pupils must immediately tell an adult, (school staff or parent) if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated with care and attachments not opened unless the author is known.
- Our schools do not encourage e-mail from pupils to external bodies unless the contact is well known.
- The forwarding of chain letters is not permitted.

Mobile phones

25. Children are not allowed to bring mobile phones to school. Under special circumstances, school leaders will grant approval for mobile phones to be brought to school, but these will be kept in the office during school hours and handed back to the child at home time. Prior permission will need to be sought by the parent/carer. (Appendix E) Any loss or damage to the device will be the responsibility of the parent/carer. Any device found in the possession

of a child in school, will be confiscated and returned to the parent at the end of the school day. Children are not allowed to take mobile phones on school trips.

Internet games

26. There are times in the week when children have 'free' use of school networks, such as during computer clubs, wet playtimes, good behaviour reward time etc. Any games played on school networks must be in line with the relevant codes of conduct and be suitable for primary children. This will be monitored by the supervising adult.

Downloading music

27. Children should not download music on to our school networks. If music is free to download, it may be illegal. Staff may download music but this must be done legally and in line with copyright laws.

Managing emerging technologies

28. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

29. The SLT should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Therefore, mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

30. The appropriate use of learning platforms will be discussed as the technology becomes available in the schools.

Internet safety skills for pupils

31. Pupils should be reminded of internet safety rules when using the internet, and will be taught:
    a. How to critically evaluate materials
    b. Good searching skills
    c. The importance of intellectual property (e.g. copyright issues) regarding materials they find on the internet.

32. E-safety forms part of our schools' Computing curriculum.

Social networking and personal publishing

33. The school filters do not allow access to major social networking sites, and pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Primary children are also below the permissible age for most social media sites.

34. Pupils are advised never to reveal personal details of any kind which may identify them, their friends or location.

Sanctions

35. Sanctions will be appropriate to the seriousness of the offence. For example, temporary suspension of ICT rights for minor offences, ranging to permanent exclusion and involvement of the police for very serious offences.

School web site

36. Any work published on our school websites is thoroughly checked to ensure that there is no content that compromises the safety of pupils and staff. The schools will not use images of pupils on the web site or in any other media if specifically instructed not to by parents/carers; a letter is sent home on induction giving parents/carers the opportunity to do so. We ensure image files are appropriately named and staff should not use pupils' names in image file names or ALT tags if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. Wherever possible, we will use group photos rather than photos of individual children. Images will be appropriately stored and secured on the school's networks.

Publishing pupils' images and work

37. Photographs that include pupils will be selected carefully with the permission of parents/guardians.

38. Work can only be published with the permission of the pupils and parents/carers.

39. Parents are clearly informed of the schools' policy on image taking and publishing, both on school and independent electronic repositories. Refer to the Volunteering in school leaflet.

Network etiquette and privacy

40. Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:
    a. Be polite – never send or encourage others to send abusive messages.
    b. Use appropriate language – users should remember that they are representatives of their school on a global public system. Illegal activities of any kind are strictly forbidden.

c. Users should not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
d. Privacy – users should not reveal any personal information (e.g. home address, telephone number) about themselves or other users, and should not trespass into other users' files or folders.
e. Password – users should not reveal their passwords to anyone with the exception of pupils sharing their login details with their parents / carers so they can access relevant online learning at home. If they think an unauthorised person has learned their password they must contact the IT Coordinator.
f. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Users should not send anonymous messages.
g. Disruptions – users should not use their network in any way that would disrupt its use by others.
h. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
i. Staff or students finding unsuitable websites through school networks should report the web address to the head of school/ school technician.
j. Users should not use unencrypted external memory devices and any device used should be checked for viruses.
k. Users should not attempt to visit websites that might be considered inappropriate – including those relating to illegal activity. All sites visited leave evidence in the county network if not on the computer.
l. Downloading some material is illegal and police or other authorities may be called to investigate such use.
m. Unapproved utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
n. Files held on the school's network will be regularly checked.
o. It is the responsibility of the user (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the internet/intranet does not occur.

Unacceptable use

41. Examples of unacceptable use include but are not limited to the following:
    a. Users must log-in with their own user ID and password, where applicable, and must not share this information with other users with the exception of pupils sharing their log-in details with their parents/carers so they can access relevant online learning at home. They must also log off after their session has finished.
    b. Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
    c. Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (Filters are in place to block e-mails containing language that is or may be deemed to be offensive.)
    d. Accessing or creating, transmitting or publishing any defamatory material.
    e. Receiving, sending or publishing material that violates copyright law. This includes through video conferencing and web broadcasting.
    f. Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
    g. Transmitting unsolicited material to other users (including those on other networks).
    h. Unauthorised access to data and resources on school network or other systems.
    i. User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

42. Users must comply with the acceptable use policy of any other networks that they access.

43. Users must not download software without approval from the IT Coordinator or SLT.

Services

44. 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.

Physical security

45. Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for

example will need to be physically protected by locks and or alarms.

Wilful damage

46. 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

47. Written permission from parents or carers will be obtained before photographs and/or names of pupils are published, and the school has a separate form for this purpose.

48. Publishing includes, but is not limited to:
    a. the school web site
    b. the Local Authority web site,
    c. web broadcasting,
    d. TV presentations,
    e. newspapers.

49. Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.

Assessing risks

50. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the schools, nor West Sussex County Council can accept liability for any material accessed, or any consequences of internet access.

51. The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

52. Complaints of internet misuse will be dealt with by the IT Coordinator or SLT.

53. Any complaints about staff misuse must be referred to the Executive Headteacher.

54. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

55. Pupils and parents will be informed of the complaints procedure (see school's complaints policy).

56. Pupils and parents will be informed of consequences for pupils misusing the internet.

This policy will be reviewed and updated annually. It will form part of induction for all new staff.

Appendix A: Pupil acceptable use policy

1. All pupils must follow the rules in this policy when using school computers.
2. Pupils who do not follow these rules may find:
    a. They are not allowed to use the computers,
    b. They can only use the computers when supervised, and
    c. They may have their username blocked for a period of time decided by staff.
3. Their teachers will show pupils how to use computers.

Unacceptable use

4. Examples of unacceptable use include, but are not limited to:
    a. Using a computer with another person's name and password.
    b. Creating or sending on the internet any messages that might upset other people.
    c. Looking at, or changing work that belongs to other people.
    d. Wasting time or resources on school computers.
    e. Trying to access inappropriate material.

What to do if you see something that concerns you

5. It is likely that at some point you will come across some images or words that you did not intend to see. If this happens and you do see something that scares, worries or upsets you, do the following immediately:
    a. Turn the computer screen off! Do not turn the PC off.
    b. Put your hand up and ask for a teacher to come straight over.
    c. DO NOT show other students what you have seen or discuss it with them.
    d. Wait for someone to come over and help you quietly.
6. The teacher will then tell you what to do next.

See appendix B for pupil acceptable use form

Appendix B: Acceptable use of ICT form

Pupil:

As a school user of the Internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school. I agree to report any misuse of the network to my teacher. I also agree to report any websites that are available on the school internet that contain inappropriate material to a member of staff.

If I do not follow the rules, I understand that this may result in loss of access to the Internet as well as other disciplinary action.

Pupil Signature: _____ Date: _____/_____/_____

INSERT SCHOOL NAME:_____

Parent/legal guardian:

As the **PARENT/LEGAL GUARDIAN*** of the pupil named above, I give permission for my child to access networked computer services such as the internet, e-mail and the school's virtual learning environment. I understand that pupils will be held accountable for their own actions. I also understand that although the school will take reasonable steps to ensure that my child is appropriately supervised, according to age and responsibility, I will not hold the school or County Council responsible for inappropriate material that my child may obtain. I understand the school reserves the right to apply monitoring arrangements to any student in relation to network, e-mail and Internet use where misuse is suspected. I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media. I agree to report any misuse of the network to the school.

- My child's work, if selected, **CAN / CANNOT*** be published on the internet, including the school and West Sussex County Council websites
- My child **CAN / CANNOT*** take part in Internet / video conferencing between the school and another institution.

Please note that this does not refer to newspaper publicity.
**** PLEASE DELETE AS APPLICABLE***

Parent/legal guardian name: _____
(Capitals please)

Parent Signature: _____
Date: _____/_____/_____

DVSF schools sadly acknowledges the increasing role that the internet and mobile technology is playing in many child protection and bullying cases across the country. Further help and advice is available for parents from CEOP at www.thinkyouknow.co.uk

Appendix C: Staff acceptable use policy

School networked resources may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

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, monitoring and/or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Conditions of use

Personal responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse or the network to the IT Coordinator or SLT.

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 our 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 DVSF schools (or West Sussex County Council) into disrepute.
2. I will use appropriate language – I will remember that I am a representative of the DVSF schools 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 IT Coordinator.
9. I will ensure that I log off after my network session has finished.
10. If I find an unattended machine logged on under other users username I will not continuing using the machine – I will log it off immediately.
11. I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the SLT.
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.
    a. I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the SLT or IT Coordinator.
    b. I will not use personal memory devices or laptops on the network without having them approved by the IT

Coordinator and checked for viruses.

c. I will not save any school files onto my private devices but will work on them via my school MS 365 account.

14. 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.
15. I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
16. 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.
17. Damage to professional reputations can inadvertently be caused by innocent postings or images - I will be careful with who has access to my pages through 'friends' and 'friends of friends', especially with those connected with my professional duties, such a school parents and their children.
18. I will ensure that any private social networking sites / blogs etc. that I create or to which I actively contribute, are not confused with my professional role in any way.
19. I will support and promote the DVSF school's e-safety and data protection / security policies and help students be safe and responsible in their use of the Internet and related technologies.
20. I will not send or publish material that violates Data Protection Act or breaches the security this act requires for personal data.
21. I will not receive, send or publish material that violates copyright law. This includes materials sent / received using video conferencing or web broadcasting.
22. I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
23. I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
24. I will ensure that any personal data (where the Data Protection Act applies) that is sent over the internet will be encrypted or otherwise secured.

See appendix D for staff agreement form

Appendix D: Staff user agreement form for internet access

As a school user of the internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. I agree to report any misuse of the network to the IT Coordinator. I also agree to report any websites that are available on the school Internet that contain inappropriate material to the IT Coordinator. 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 SLT.

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 (please print): _____

Signature: _____ Date: _____/_____/_____

INSERT SCHOOL NAME:_____

Appendix E: Permission for a child to Bring a Mobile Phone to School

I wish to apply for permission for my child _____

to bring a mobile phone to school on (date or state 'every day') _____.

The reason for this request is:

I understand that the device will be kept in the school office and returned to my child at home time.

I understand that the school will not be held responsible for any loss or damage to the device.

Parent/carer name:_____

Parent/carer signature: _____ Date:_____

To be completed by school leader. Please copy and return to parent/carer.

I give/do not give permission for:

_____ to bring their own mobile phone to school on the above dates, provided the agreed conditions are met.

If permission is not given, state reason.

SLT signature: _____