Acceptable Use Policy

Eastergate C.E. Primary School

Adopted by the Full Governing Body
14th November 2018
Review Date: November 2019

Introduction

This document sets out the Acceptable Use Policy for Eastergate CE Primary School. There are adaptations of the policy for the various Key Stages as well as one for the Staff, Volunteers and Governors.

Access to the school I.T. network is a privilege for all users and should not be regarded as an automatic right. All users must follow the conditions described in this policy when using the school network.

For pupils, teachers will show them how to safely use the resources available through the IT systems. Staff and other users can receive advice from the Headteacher.

The network will be checked regularly to make sure that it is being used responsibly by all.

The school will not be responsible for any loss of data or work as a result of the system or user mistakes in using the system.

The use of any information gathered via the network and the school internet connection is at the user's own risk.

This Acceptable Use Policy also includes the use of any other IT devices, mobile phones and cameras and including any social media forms and network sites, where any direct or indirect reference is made regarding EGPS, pupils or staff or work related matters.

Users that do not adhere to the policy may face the following sanctions:

- Close monitoring of their school network activity
- Detailed investigation of their past school network activity
- Withdrawal of network access privileges
- Behaviour investigation - pupils
- Disciplinary investigation - staff
- In some cases, criminal prosecution

Acceptable Use Policy (AUP)

The 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 network will only be permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Our overarching Network etiquette and privacy rules

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be seen as bullying, discriminatory or calculated to incite hatred against any person or group of persons, including ethnicity, religion or other person or group with a protected characteristic.
- Privacy – do not reveal any personal information (for example date of birth, home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Password – do not reveal your password to anyone. If you think someone has learned your password then contact member of staff responsible
- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.
- Users will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
- Users finding unsuitable websites through the school network should report the web address to the school IT manager.
- Do not introduce any USB drives, data disc or other portable devices into the network without having them checked for viruses.

- Do not use personal devices to transfer data or pictures of a non-educational nature onto the school IT system.

- Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.

- Files held on the school's network will be regularly checked by the member of staff responsible.

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 or intranet does not occur.

Pupil Acceptable Use Policy EYFS and Key Stage 1

All pupils must follow the rules in this policy when using school computers, and the school cloud services. Pupils that do not follow these rules may find:

- They are not allowed to use the computers.
- They can only use the computers if they are more closely watched.
- Their teachers and school staff will show pupils how to use the computers, help them understand the rules and will supervise their use of the computers.

Computer Rules

1. I will only use polite language when using the computers.

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

3. I know that my teacher or staff will regularly check what I have done on the school computers.

4. I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.

5. I must not tell anyone my name, where I live, or my telephone number over the Internet.

6. I must not tell my username and passwords to anyone else but my parents.

7. I must never use other people's usernames and passwords or computers left logged in by them.

8. If I think someone has learned my password then I will tell my teacher.

9. I must log off after I have finished with my computer.

10. I must not use the computers in any way that stops other people using them.

11. I will report any websites that make me feel uncomfortable to my teacher or a member of staff.

12. I will tell my teacher or a member of staff straight away if I am sent any messages that make me feel uncomfortable.

13. I will not try to harm any equipment or the work of another person on a computer.

14. If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

Unacceptable Use

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Waste time or resources on school computers.

Pupil Acceptable Use Policy – Key Stage 2

Pupil access to the school network and cloud services is a privilege, not a right. All pupils must follow the conditions described in this policy when using the school network, Internet access and the school cloud services.

Pupils that do not follow these conditions may face:

- Withdrawal of the access,
- Monitoring of the network activity,

- Investigation of past network activity

Pupils will be shown by their teachers how to use the resources available through the school's network. School staff will regularly check the network to make sure that it is being used responsibly.

The school will not be responsible for any loss of data or work as a result of any system faults, errors, or pupil mistakes in using the system. The use of any information gathered via the network and the school Internet connection is at the pupil's own risk.

Conditions of Use

Pupils will be expected to use the school network system for the purposes for which the school provides it. It is the personal responsibility of every pupil to take all reasonable steps to follow the conditions set out in this Policy. Pupils must also accept personal responsibility for reporting any misuse of the network to the Headteacher.

Acceptable Use

Pupils are expected to use the network systems in a responsible manner. It is not possible to provide a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the school ethos. The following list does provide some examples that must be followed:

1. I will not create, send or post any material that is likely to upset or offend other people or give the school (or West Sussex County Council) a bad name.

2. I will only use appropriate language – I will remember that I am representing the school on a public system

3. I will not use language that could stir up hatred against any ethnic, religious or other minority group.

4. I realise that members of staff will regularly check files held on the school network.

5. I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.

6. I will not trespass into other users' files or folders.

7. I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.

8. I will ensure that if I think someone has learned my password then I will tell my class teacher.

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 users' username I will not continue using the machine – I will log it off immediately.

11. I understand that I will not be allowed access to unauthorised chat rooms and should not attempt to gain access to them.

12. I am aware that email is not guaranteed to be private. Messages supporting illegal activities will be reported to the authorities. Anonymous / unnamed 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 to other people's information or unsuitable websites that make me feel uncomfortable to my class teacher.

15. I will report to the ICT Manager immediately if I am sent any messages or materials that make me feel uncomfortable.

16. I will not introduce "USB drives" or other portable devices into the network without having them approved and checked for viruses.

17. I will not try to visit websites that might be inappropriate or illegal. Downloading some material is illegal and I know the police or other authorities may be called to investigate if this were done.

18. I will not download or install any unapproved software from the Internet.

19. I realise that pupils under reasonable suspicion of misusing the network may have their usage closely monitored or have past use investigated. Illegal activities of any kind are strictly forbidden.

20. I will not receive, send or publish material that violates copyright law.

21. I will not attempt to harm any equipment, work of another user, or another website connected to the school system.

22. I understand that unapproved software and executable files (eg programs downloaded from the Internet) are not allowed in my work areas or attached to e mails.

23. I agree to follow the acceptable use policy of any other websites or networks that I access.

Unacceptable Use

Examples of unacceptable use include, but are not limited to:

- Logging in with another person's user ID and password, or using a machine left unattended but logged on by another user.
- Creating, sending, or posting on the Internet any material (text, images or sounds) that is likely to upset other people or cause offence.
- Unauthorised access to resources and work that belong to other "users".
- Pupil activity that would:
    - Cause damage to, or destroy other users' work,
    - Go against the privacy of other users,
    - Deliberately waste time or resources on the school network,
    - Result in damage of school computer equipment

Network Security

If you discover a security problem, for example being able to see other pupil's work areas, you must inform your class teacher. Pupils identified as persistently failing to adhere to this policy will not be allowed to access the network.

Staff, Volunteers and Governors Acceptable Use Policy

School networked resources, including cloud services, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. 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. Users 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 of the network to the Head Teacher. All users should ensure any transfer or sharing of data is in compliance with the Data Protection Act.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All school computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

This includes the use of any other IT devices, mobile phones and cameras and including any social media forms and network sites, where any direct or indirect reference is made regarding EGPS, West Sussex County Council, pupils or staff or work related matters.

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, upload to the school systems or publish any illegal material or 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 not use school network, or school devices to access or receive material that would not be considered suitable for a general audience

3. 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.

4. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

5. I understand that users under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

6. 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 pupils.

7. I will not trespass into other users' files or folders.

8. 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. I will choose appropriate, secure passwords, and change these regularly (at least half-termly).

9. I will ensure that if I think someone has learned my password then I will notify the Headteacher.

10. I will ensure that I log off after my network session has finished.

11. If I find an unattended machine logged on under other user's username I will not continue using the machine – I will log it off immediately.

12. 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 school leadership team, and images should be removed from the device immediately after upload. We do not expect this type of use to occur within the school site as devices are provided for this use. Personal devices should be stored away from pupils during the school day.

13. I am aware that email 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.

14. I will not use the network in any way that would disrupt use of the network by others.

15. I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Headteacher.

16. 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.

17. 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. I understand that I must not use alternative internet connections (eg mobile networks) to attempt to gain access to sites or materials that would be blocked on the school system.

18. I will not download any unapproved software, system utilities or resources from the Internet. These might compromise the network or not be adequately licensed.

19. I will not accept invitations from children, young people or parents/carers of pupils 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, such a school parents/carers and their children.

20. 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. I will not harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.

21. 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.

22. I will not send or publish material that violates the Data Protection Act or breach the security this Act requires for personal data

23. I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting. I will also refrain from using or storing any materials in breach of copyright law on the school network.

24. I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

25. I will ensure that portable IT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

26. 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.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users can access range of resources to support digital technologies at https://swgfl.org.uk/products-services/online-safety/resources/digital-literacy

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 Headteacher immediately if a security problem is identified and should not demonstrate this problem to other users. Users identified as a security risk will be denied access to the network.

Media Publications

Written permission from parents or carers must be obtained before photographs or named photographs of students are published. Further guidance can be found in the "West Sussex County Council Photographic Images of Children Guidelines" February 2015.