Acceptable Use Policy

1 Preface

This document sets out the Vale School's Acceptable Use Policy. 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 and the school 'cloud services' 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, and school cloud services.

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 school IT manager.

School staff will regularly check the network to make sure that it is being used responsibly by all. Formal checks of data on the system will be conducted at least monthly.

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 the Vale School, pupils or staff or work related matters.

Users that do not follow 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 computer systems are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any use of the systems that would bring the name of the school or County Council into disrepute is not permitted.

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 systems will only be permitted upon receipt of signed permission and agreement forms. There are three AUP documents covering Early Years/KS1, KS2 and Adults.

All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion and formal checks will be carried out on stored data at least monthly.

Our overarching principles and privacy rules for ICT.

Users are expected to abide by the school's principles and rules for the use of ICT. These rules include, but are not limited to, the following:

Do not use the system in connection with illegal activities of any kind.

Use appropriate language – users should remember that they are representatives of the school on a global public system.

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.

Do not reveal any personal information (for example date of birth, home address, telephone number) about yourself or others.

Do not trespass into other users' files or folders.

Do not reveal your password to anyone. If you think someone has learned your password then contact the IT Manager.

Electronic mail is not guaranteed to be private. Users must adhere to the school Data Protection protocols and policies for the sending of data. Do not send anonymous messages.

Do not use the network in any way that would disrupt use of the network by others.

Do not attempt to visit websites that might be considered inappropriate. Downloading some material is illegal and the police or other authorities may be called to investigate such use. Users finding unsuitable websites through the school network should report the web address to the school IT manager immediately.

Do not use any USB drives, data disc or other portable devices on school machines.

School Personal Data must not be transferred to personal devices or personal accounts.

Unapproved software and programs cannot be used.

Data held by individuals on the school's network will be subject to formal checks, at least monthly, 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 system does not occur.

2. Pupil Acceptable Use Policy - EYFS and Key Stage 1

This policy is written for the parents to share with their children in these year groups.

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.

2.1 Computer Rules

- Before I write anything I will ask myself "Is it necessary, kind and true?”
- I will tell my teacher or another member of staff if:
  - I see things on a website that I don’t like
  - I am sent a message that I don’t like
- I must not tell anyone my name, where I live, or my telephone number on the computer.
- If my teacher gives me a password, I must not tell anyone else but my parents.
- I will not try to damage any equipment, or delete or change another person’s work.
- I must log off after I have finished with my computer.
- I know that my teacher or staff will regularly check what I have done on the school computers, and if they think I have been breaking the rules they will check on how I have used the computers before.

You may not be allowed to use the computers if you do not follow all of the above rules.

3. Pupil Acceptable Use Policy – Key Stage 2

Pupil access to the school IT systems and cloud services is a privilege, not an automatic right.

All pupils must follow the rules described in this policy when using the school computers, Internet access and the school cloud services.

Pupils that do not follow these rules may:

- Not be allowed to use the computers
- Be watched more closely when using computers
- Have their past use of the computers looked at closely

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

3.1 Conditions of Use

Pupils will be expected to use the school computer system for the purposes for which the school provides it. It is the responsibility of every pupil to follow the rules set out in this Policy. Pupils must also accept responsibility for reporting any misuse of the system to the IT Manager.

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 system and the school Internet connection is at the pupil's own risk.

3.2 School Rules for IT

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

- I must not share my usernames and passwords with anyone else except my parents.
- If I think someone has learned my password then I will tell my teacher or the IT Manager.
- I must never use other people's usernames and passwords or computers left logged in by them.
- Before I write anything I will ask myself "Is it necessary, kind and true?"
- I must not talk to other people outside of the school online without permission from my teacher.
- I will not tell anyone my name, where I live, my telephone number, or other information about myself or my family online.
- I will tell my teacher or another member of staff if:
  - a website makes me feel uncomfortable
  - I am sent a message that makes me feel uncomfortable
  - I see something on the internet I shouldn't see
- I must not try to access any areas on the computer or websites which the system does not allow me to. I understand that downloading some things can be illegal. I know the Police could be called to investigate any illegal activities.
- I will not download or install any programs.
- I will not damage any equipment or systems, and I will not do anything on the computers that will stop other people from using them.
- I must not access work that belongs to other people without permission from my teacher.

- I must not use any USB drives, portable devices or a mobile phone whilst in school.
- I will not receive, send or publish any computer files that are protected by copyright law. This means that I will not attempt to download or copy music, movies, videos, pictures or written work that I have not created without permission from my teacher.
- I must log off after I have finished with my computer, and if I find a computer that someone else has left logged-on, I will log it off immediately and tell my teacher.
- I know that my teacher or staff will regularly check what I have done on the school computers and if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.

3.3 Examples of things that I must not do:

- Logging in with another person's user ID and password, or using a machine left 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.
- Any activity that would:
    - Cause damage to, or destroy other users' work
    - Deliberately waste time or resources on the school system
    - Result in damage of school computer equipment

3.4 Security

If you discover a security problem, for example being able to see other pupil's work areas, you must tell your class teacher or the IT Manager. If you fail to follow the school rules, you will not be allowed to use the computers.

Staff, Volunteers and Governors Acceptable Use Policy

School IT systems, including cloud services, are intended for educational purposes, and may only be used for legal activities consistent with the rules of 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, monitoring and / or retrospective investigation of the user's use of services, in accordance with the relevant Disciplinary Policy and/or Codes of Conduct. In some instances, misuse could lead to criminal prosecution.

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 IT systems, or security problems with the systems to the IT Manager or Head Teacher. All users should ensure any transfer or sharing of data is in compliance with the General Data Protection Regulation.

Acceptable Use

Users are expected to utilise the IT systems in a responsible manner. All 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, where any direct or indirect reference is made regarding the Vale School, 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 use the IT systems in connection with illegal activities of any kind.

2. I will not use the school IT systems or devices to access or receive material that would not be considered suitable for a general audience.

3. I will not use language, or create, transmit, display or upload material to the school systems, or publish material that is likely to:
    - Harass any person
    - Cause offence
    - Cause inconvenience or needless anxiety
    - Incite hatred against any ethnic, religious or other group
    - Promote extremist political or religious views
    - Reflect negatively on the school or West Sussex County Council
    - Bring the school or West Sussex County Council into disrepute

4. 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.

5. Security
    - I will not use the IT system in any way that would disrupt use of the network by others.
    - I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the IT Manager.
    - I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
    - I will not trespass into other users' files or folders.
    - I will not download any unapproved software, system utilities or resources from the Internet. Any new software or systems must be discussed with the IT Manager before use.
    - 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. I will not use accounts belonging to other users. I will choose appropriate, secure passwords at least (eight characters in length, upper and lower case with numbers, no obvious words or names), and change these regularly (at least half-termly). I will use two-factor verification methods to secure my Google account. I will not repeat passwords between different systems.
    - I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the IT Manager.
    - I will ensure that I lock my computer when temporarily leaving the room, and will log off at the end of the session. If I find an unattended machine logged on under another user's. username I will not continue using the machine – I will log it off immediately.
    - Staff with access to central school account passwords must store these within the designated password management system.

6. Data Protection
    - I will not reveal any personal information (e.g. home address, telephone number, e-mail addresses) of other users to any unauthorised person. I will not reveal any of my personal information to pupils.
    - I will ensure that any Personal Data that is sent outside of the school will be encrypted or otherwise secured, in compliance with the General Data Protection Regulation. Where provided, secure messaging systems should be used to transfer such information.
    - I am aware that e-mail is not guaranteed to be private. Personal Data must never be included in the subject line of any e-mail.
    - I will use the BCC: field for e-mail addresses when sending e-mails to groups of unconnected individuals.
    - I will not forward my school e-mail to a personal account, or any third-party.
    - I will support and promote the school's e-safety and Data Protection policies and help students be safe and responsible in their use of the Internet and related technologies.

7. Social Media
    - I will not use social media to publish negative personal opinions of the school or the County Council, and I will not post any material likely to bring the school or the County Council into disrepute. I understand that any public postings must not be inflammatory, derogatory or contain abusive language.
    - I will not accept invitations from pupils to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. Staff must be aware that social media links with parents/carers of children at the school can carry a risk of damage to professional reputations and the image of the school, which can be inadvertently 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.
    - 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.

8. Devices
    - I will not use personal digital cameras or camera phones for creating or transferring images of children and young people.
    - Personal devices must be stored away from pupils during the school day.
    - I will ensure that smartphones used to access my Google account are protected with PIN, fingerprint or equivalent security measures and that other people do not have unsupervised access to the device. I will ensure that my account is removed from the phone when disposing of it.
    - I will ensure that school portable IT equipment such as laptops, digital cameras are securely locked away when they are not being used.
    - I will not use USB drives, portable hard-drives or personal laptops on the school system.
    - I will not download any personal data onto a personal device or USB drive

9. 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.

10. 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, which may lead to disciplinary action.

Additional guidelines

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

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.

Cloud services are dependent on servers, connections and equipment which are outside of the control of the school. The availability of these systems, and any errors, data loss or corruption that may occur through the use of these systems, are the responsibility of the service providers and are subject to their standard terms of use. Users are reminded that data stored on Cloud services is not backed up by the school and recovery options will be limited in the event of accidental deletion or corruption of such data. The Google Apps terms of service can be reviewed at
http://www.google.co.uk/apps/intl/en-GB/terms/education_terms.html

Media Publications

Written permission from parents or carers must be obtained before photographs or students' work is published.

References

The following hard copies are held centrally.

- West Sussex Guidance for the Safer Use of the Internet by Staff Working with Young People.
- West Sussex County Council Copyright Information for Schools

The text of sections 2 and 3 are reproduced in the relevant Admissions Forms and must be updated in line with this policy when changes are made.