



E-SAFETY AND PUPIL ACCEPTABLE USE POLICY

Date: 2018/2019

e-Safety and Pupil Acceptable Use Policy (AUP)

This policy sets out the rules for pupils when using Falinge Park High School's computers, systems, shared areas and communication services (online and otherwise), and also applies when accessing these from outside school. Collectively, these resources are referred to as the 'school network'. This has been established to support the delivery of a compelling learning experience and high quality teaching and learning.

School computers, devices or equipment must only be used for 'educational purposes' which benefit learning, purposeful communication and research. Pupils must only use programs which have been approved and installed onto the network by IT technical staff.

The following are strictly forbidden:

- use of the school internet access or systems (including email) to offer, provide or purchase products or services
- use of personal computer devices or online services to attempt to gain unauthorised access to the school network

Pupils may use personal storage devices (i.e. USB Memory Sticks) to transfer work between home and school, provided these are used solely for school work and are kept free from viruses. School reserves the right to apply the same monitoring and controls imposed on the school network to these.

Network accounts, Pupil Internet, VLE, Email and Home access (Desktop Anywhere)

Pupils will be given a network account with a unique username and password. This will allow users to save all school-work into their own personal area, within the school network.

Pupils will have access to the internet (this is filtered for safety reasons), access to the school's online teaching and learning portal which includes Google Drive and Google Classroom) and a secure web-based email service for school-work related purposes.

There is also 'Desktop Anywhere' which offers an out-of-school, secure, direct link into a pupil's own network account and the shared network areas whilst away from school. This can be accessed via the 'Services' section of our school website using any computer or device with an internet connection. Pupils then log into 'Desktop Anywhere' using their network username and password – as though in school.

Network accounts and the use of resources and equipment will be monitored. Misuse of resources or equipment, or breaking the rules of this policy will result in sanctions being applied. User accounts may be suspended, network access restricted plus additional sanctions as described later in this policy. In the event of account suspension or network

restrictions users must see the IT technicians to discuss this as soon as they are notified.

Personal Responsibility Pupils MUST be aware of the following:

- You are responsible for setting and safeguarding your own username and **STRONG** passwords, and for informing the IT technical staff if you suspect another person knows it. You must **NEVER** allow anyone else to use your login and password
- Your activity on the network is logged automatically and continuously. This includes details about the workstations you use, how long you are logged on for, the software used, email messages sent and the websites you search and view – this is to keep you, other users and the network safe
- You are expected to report any violation or breach of the e-Safety and AUP policy through the “report abuse button” on the start menu. This will be sent through to the director of IT (Mrs L Thompson) who will take appropriate action
- Details of any unacceptable material, email or internet browsing will be recorded and your access to the network and systems suspended. Your parents/guardians may be notified or asked to come into school to discuss the matter further. This could also result in an escalation of sanctions dependent on the nature of the breach
- Video, audio or photographic recording of staff or pupils for activities other than those authorised by the school, is **strictly** forbidden

Personal Safety

Pupils **must** take care to keep their own and other user’s personal information private. They must not electronically share (online or otherwise) information about their own or another person’s address, telephone number(s), email address or photographs. Permission **must** be sought from another person before sharing any content relating to them.

Policy Violations

The school will cooperate fully with local or government officials in any investigation related to any illegal activities conducted through the school network.

Misuse of any of the school’s systems or services will be dealt with inline with the **Compelling Behaviour** policy. This will involve your class teacher applying an appropriate sanction and entering this in to your school record. In cases of continued misuse/breach or incidents deemed to have a significant impact on teaching and learning or the safeguarding of pupils and staff, these will be reported to the Head of Year who will escalate and address inline with the compelling behaviour policy.

Infringements of this policy may result in one/a combination of the following sanctions:

- Senior detention, interview and/or counselling by Tutor/Head of Year/e-Safety Coordinator or Headteacher
- Re engaging and support understanding the breach related to e-Safety and/or accessible us policy

- Informing parents or carers and potentially inviting them into school for further dialogue and support
- removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
- Period of time in reflection or fixed term exclusion
- Referral to Local Authority and/or Police

Examples of violations include when you:

- knowingly share your username and password(s) with another person
- put programs into your network storage area or network areas (incl. online areas)
- store, create or share unnecessary or inappropriate files (images, music, video, etc.)
- store, create or share files that cause reason for concern
- use the computers irresponsibly, in a way that causes concern or disrupts teaching and learning
- vandalise computers or any other IT resources
- use computers for non-educational purposes or when not instructed
- knowingly attempt to access sites containing material which are deemed inappropriate such as those that contain sexist, pornographic, homophobic, racist, extremist/radical or offensive content
- use the internet in a way that causes concern or disrupts teaching and learning, including sites which encourage disruption of the network or its ability to protect users
- create, send or forward 'junk' messages not related to school work or school matters
- use email in a way that causes concern or disrupts teaching and learning including the use of group emails
- use unauthorised communication services such as email and instant messaging

Discretionary Rights: The school reserves the right to vary the terms of this policy without prior notice. Additionally, to withdraw a user's access to the network and other services. The decision of the school is final.

Useful Websites: Our school website www.falingepark.com contains useful information and advice regarding e-Safety via the information tab. We recommend that parent/guardians use this section of our site to find out more.

KEEP THIS DOCUMENT FOR YOUR OWN INFORMATION



Pupil Acceptable Use Policy – Reply Slip

Please complete and return to School.

Keep the Policy for your own reference.

Pupil Agreement:

I agree to comply with the rules in the Acceptable Use Policy. I will conduct myself in a responsible way and observe all the restrictions explained to me. I understand I have a responsibility to check I understand all of the rules and to keep myself and others safe.

Pupil Name: _____

Pupil Signature: _____ **Date:** ____ / ____ / ____

Parent/Carer Agreement:

I grant permission for my child to use the school network, systems and online services. I understand they will be held accountable for their own actions and that some materials on the internet may be objectionable. I support the school and will set standards for my child to follow when selecting, sharing, using and exploring information and media at home.

Parent/Carer Signature: _____ **Date:** ____ / ____ / ____