Below are some answers to the questions the Online Safety team get asked most frequenty. If you have a question that is not anwered here, please contact us at enquiries@swgfl.org.uk.

What is the headteachers responsibility?

The Headteacher is responsible, through the legal duty of care, for ensuring that all pupils and staff are safe. This includes protecting staff and pupils from the dangers associated with electronic communications.

It is the duty of the Headteacher to ensure that all staff are aware of the possible dangers associated with electronic communications, and the means for ensuring safe usage. The head teacher may, however, delegate day to day management of e-safety issues to a member of staff who is sufficiently knowledgeable, trained and competent.

It is also the responsibility of the governing body to ensure that policies are followed to ensure the safety of the school community.

Access our Online Safety Resources (http://swgfl.org.uk/products-services/esafety/resources)

What do you mean by electronic communications?

Electronic communications encompass internet technologies such as: The World Wide Web, Chat rooms, E-mail, Instant messaging, Blogs, Social sites.

Digital photography, video and sound recording can also be captured and copied to portable players (MP3 players, iPods etc). Mobile phones provide similar functions through texting, taking and sending photos and video clips. Handheld computing devices also combine many of these technologies.

All of these technologies make a positive contribution to the world and education, but all are equally capable of being abused.

What are the risks that pupils face?

If precautions are not taken, these technologies can expose pupils to hostile individuals, including sexual predators, who can form relationships with pupils, sometimes using false identities or posing as a child. This is known as grooming.

The technologies can expose pupils to pornography and pornographers, to materials extolling violence, drugs or prejudice hatred. The technologies can also enable bullying.

What are the risks for school staff?

There have been cases reported of adults being bullied or harassed at work through these technologies.

It is also the case that the school environment can provide some adults with the opportunity to exploit the technologies for their own inappropriate purposes. These include downloading or publishing offensive or illegal materials and initiating improper contacts with young people.

Staff are also vulnerable if they are singly responsible for the administration of passwords and filtering.

What should I do if I suspect or discover illegal activity on the web?

Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the police.

It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police.

Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the internet safety co-ordinator, network manager or headteacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

It is essential that evidence is preserved.

What do I do if I suspect or discover unacceptable activity?

Follow the agreed course of action in your Acceptable Use Policy (AUP).

If there is no specific reference to help you in your AUP, you may find support in your Anti-bullying Policy or PSHE Policy.

What steps can the Headteacher take to ensure that pupils and staff are safe?

Ensure that:

- The headteacher and all staff and governors are familiar with the risks and precautions.
- All pupils are made aware of the dangers of electronic communications, of the precautions that they can take and of how they can report unsafe activity.
- An Acceptable Use Policy (AUP) for staff and pupils is in place. This policy will describe risks, precautions and procedures and must be signed by all staff, parents and guardians. It should also be drawn to the attention of all governors.
- The school has a code of good practice, written in a way which pupils can understand, that is displayed prominently and, when pupils are of an age to appreciate the significance, signed by them.
- A secure route for reporting any bullying or unacceptable behaviour is established and understood by the whole school community.

What is the difference between unacceptable and illegal use of the internet?

Illegal usage includes:

- Making, producing or distributing indecent images of children.
- Grooming.
- Making, producing or distributing adult material that breaches the Obscene Publications Act in the UK.
- Accessing, downloading or forwarding criminally racist material.
- Any activity using technology to cause serious harassment, anxiety, alarm or distress which may be contrary to the Harassment or Malicious Communications Acts.

Unacceptable use includes:

- Making, producing or distributing any materials that are in conflict with the ethos of the school. This will include materials that, while not illegal, contain gratuitous sexual or violent content, incite hatred or which encourage the use of illegal drugs.
- Staff using the school infrastructure for personal reasons during contact time.

Can the headteacher delegate responsibility for e-safety in their school?

No, the headteacher is always responsible. The authority to manage e-safety and day to day monitoring can be delegated to members of staff who are sufficiently knowledgeable, trained and competent.

It also protects staff if there's more than one person who takes part in the monitoring of activity on the school network.