IT User Agreement

School staff are responsible for ensuring that:

• they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
• they have read, understood and signed the school guidance for 'Safer-working Practice for Adults who work with Children and Young People'
• they report any suspected misuse or problem to the Online Safety Officer for investigation and action
• digital communications with students should be on a professional level and only carried out using official school systems
• students understand and follow the School Online Safety and Acceptable Use Policies
• they monitor ICT activity in lessons, extra-curricular and extended school activities
• they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices (see Handheld Devices and Mobile Phone information below)
• in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Use of digital and video images – photographic and video:

• When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet e.g. on social networking websites.
• Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students must not take, use, share, publish or distribute images of others without their permission.
• Photographs published on the school's website, or elsewhere, that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Parents or carers are given the opportunity to withdraw photographs of students that are published on the school website.

Communications:

When using communication technologies the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored. Users need to be aware that email communications may be monitored (see Code of conduct Policy).
• Users must immediately report, to the Online Safety Officer or designated officer for child protection – in accordance with the school policy - the receipt of any email that makes them feel uncomfortable and/or is offensive, threatening or bullying in nature. They must not respond to any such email.
• Any digital communication between staff and students or parents/carers (email, VLE etc.) must be professional in tone and content.

Unsuitable / inappropriate activities:

Users shall not visit internet sites, post, download, upload, communicate or pass on, material and comments that contain or relate to:

• offensive materials: child sexual abuse images, promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation, adult material that potentially breaches the Obscene Publications Act in the UK, racist material, pornography, promotion of any kind of discrimination, promotion of religious hatred, threatening behaviour
• using school systems to run a private business
• use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and/or the School
• uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
• revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
• creating or propagating computer viruses or other harmful files
• carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet

Responding to incidents of misuse

Any apparent or actual misuse which appears to involve illegal activity, i.e.
• child sexual abuse images
• adult material which potentially breaches the Obscene Publications Act
• criminally racist material
• other criminal conduct, activity or materials will be reported initially to the Online Safety Officer.

Actions will be followed in line with the school procedures, including reporting the incident to the police and the preservation of such evidence. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Such incidents of misuse will be dealt with through the normal behaviour management policy.

Staff use of personal devices

• Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
• Staff will be issued with a school phone where contact with students, parents or carers is required.
• Mobile phones and personally-owned handheld devices will be switched off or switched to 'silent' mode during the school day. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally owned handheld devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
• Staff should not use personally-owned handheld devices, such as mobile phones or cameras, to take photos or videos of students. They should only use work-provided equipment for this purpose.
• If a member of staff breaches this school policy then disciplinary action may be taken.
• Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide their own mobile number (by inputting 141) for confidentiality purposes.

Personal use of social media

In order to safeguard your reputation and the reputation of the school, you are required to follow these guidelines in your personal use of social media.

- You must not have contact through any personal social media with a student from this school or any other school.
- You must decline 'friend requests' from students that you receive to your personal social media accounts. If you receive requests from students who are not family members, you should discuss these in general terms in class and encourage students to become 'friends' of the official school site
- Information that you have access to as part of your employment, including personal information about students and their family members, must not be discussed on your personal social media.
- Photographs, videos or any other types of images of students and their families must not be published on your personal social media.
- School email addresses must not be used for setting up personal social media accounts or to communicate through such media.

Guidance for your own privacy and safety

- You are advised to set the privacy levels of your personal accounts as strictly as you can and opt out of public listings on social networking sites.
- You should keep your passwords confidential and change them frequently.
- You should be careful about what you post online; it is not advisable to reveal home addresses, telephone numbers and other personal information.