REIGATE GRAMMAR SCHOOL

Acceptable Use Policy – Staff

Including use of Mobile Devices

ISI Code:	Acceptable Use Policy – Staff
Policy Author:	Brendan Stones, Deputy Head
Date Reviewed By Author:	June 2019
Next Review Due:	June 2021
Date Approved By Governing Body:	24 June 2019
Next Review by Governing Body Due:	June 2021

Scope of this Policy

This Acceptable Use Policy applies to staff of Reigate Grammar School. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online Behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the School's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Mobile Devices

Mobile device technology has advanced significantly over the last few years and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile devices, enabling access to a wide range of new content and services globally. Many devices (which includes mobile phones, tablets, iPods, laptops, smart watches etc.) now offer internet and email access, alongside the most often used standard functions of messaging, camera, video and sound recording.

Statement

It is recognised that it is the enhanced functions of many mobile devices that cause the most concern, and which are most susceptible to misuse, including taking and distribution of indecent images, exploitation and bullying.

It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others.

When mobiles phones are misused it may impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all.

It is appreciated that it may be very difficult to detect when such devices are present or being used, particularly in relation to enhanced functions, such as cameras. The use of all mobile phones is therefore limited, regardless of their capabilities. The aim is to avoid distraction and disruption of the working day, and to minimise the opportunities for any individual to make any covert images or misuse functions in any other way.

Designated 'mobile free' areas situated within the setting are:

- Changing areas
- Toilets

A zero-tolerance policy is in place with regards to the **use** of personal or work-related devices by any individual in these areas.

Code of Conduct

A code of conduct is promoted with the aim of creating a cooperative workforce, where staff work as a team, have high values and respect each other; thus creating a strong morale and sense of commitment leading to increased productivity. It is therefore ensured that all practitioners:

- have a clear understanding of what constitutes misuse.
- are vigilant and alert to potential warning signs.
- know how to minimise risk.
- avoid putting themselves into compromising situations which could be misinterpreted and lead to possible allegations.
- understand the need for professional boundaries and clear guidance regarding acceptable use.
- are responsible for self-moderation of their own behaviours.
- are aware of the importance of reporting concerns promptly.

It is fully recognised that studies consistently indicate that imposing rigid regulations and/or bans on the actions of others may be counterproductive, leading to a culture of suspicion, uncertainty and secrecy.

The imposition of rigorous, inflexible rules is therefore avoided, unless the potential risks of not enforcing them far out-weigh the benefits. An agreement of trust is therefore promoted regarding the carrying and use of mobile phones within the setting environment, which is agreed to by all practitioners.

Procedures

Personal devices

Effective guidance is in place to avoid the use of mobile phones causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice is promoted to protect against potential misuse. In the interests of equality, and further to promote safety, the guidance applies to any individual who has a mobile device on site, including children, parents and visitors, as detailed below:

Staff, volunteers, peripatetic teachers, supply teachers, trainee teachers and visitors are permitted to have their mobile phones with them; however, all personal use is limited to allocated lunch and/or other staff breaks, or non-contact periods when staff are not with children. It is recognised that mobile phones provide direct contact to others, and at times provide a necessary reassurance due to their ease of access, particularly at stressful times. In addition, they may enhance our own wellbeing and peace of mind, reduce stress and to enable more effective concentration on work.

It is ensured at all times that the landline telephone remains connected and operational, except in circumstances beyond the school's control. This means that it is available for emergency/urgent contact at all times.

Personal calls and texts must not be taken or made during lesson time, nor should staff be on social media sites.

Any individual bringing a personal mobile device into the setting must ensure that it contains no inappropriate or illegal content.

Use of cameras/videos to record images of children

Staff receive thorough safeguarding training and understand the significance of their role in protecting the images of children. We recognise that capturing pupil memories through photos can play an important part in celebrating everyday successes, achievements and milestones in a child's life.

There are staff cameras and staff mobile devices with a camera/video function which may be borrowed and used for events and trips, such as sporting matches or educational visits. These devices should be signed out and after the event/trip, any unwanted photos/films should be deleted immediately. The device should be returned, where any remaining photos will be uploaded to SharePoint and then deleted from the device.

At no time should any images be stored on personal devices and images **MUST NOT** be shared beyond the school community. Images may sometimes be used on the school website, twitter accounts, Facebook and other marketing materials. Parents give permission for this on entry to the school.

Staff, volunteers, peripatetic teachers, supply teachers, trainee teachers and visitors are not permitted to use their own personal devices for contacting children, young people and their families within or outside of the setting unless authorised by a member of the SLT or in the case of an emergency. This should be recorded with a member of SLT after the event.

Work Device

The use of a designated work device is promoted as it is:

- an essential part of the emergency toolkit which is taken on off-site trips.
- an effective communication aid, enabling text, email messages and calls to be made and received.
- a back-up facility should problems be experienced with the landline or where contact needs to be made outside of work hours.
- a means for staff to take photos of memory making moments to be shared with parents and the school community

Effective security measures are in place to safeguard against any potential misuse. Only authorised individuals who have received appropriate safeguarding training have access to the work device, stored securely when not in use.

Personal calls are not permitted to be made on the work mobile, other than in agreed exceptional circumstances. Contact or calls may be made via the work mobile in the event of an emergency. All calls are logged.

The work mobile is clearly labelled as such.

Driving

If any practitioner is required to drive in a working capacity, and has responsibility for the work mobile, the phone must be switched off whilst driving. The same rules apply for a member of staff's own personal mobile devices when driving. Under no circumstances should practitioners drive whilst taking a phone call. This also applies to hands-free and wireless connections, which are considered a distraction rather than a safer alternative.

Compliance with Related School Policies

This should be read in conjunction with the school's Online Safety Policy and the Staff Code of Conduct.

Breaches of this Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the **Designated Safeguarding Lead(s) (Miss Arthur, Mrs Collins, Mr Lobb, Dr Stones or Mr Boothroyd)**. Reports will be treated sensitively.