Queenswood

Electronic and Social Media Policy

Issued by	Head of IT Systems
Last review	September 2018
Circulation	Queenswood Website Governor Portal Staff Portal
Revision	i

Electronic and Social Media Policy

(Incorporating Email, Internet, Mobile Phone and Social Media Acceptable Use Policies)

Policy statement

Queenswood is committed to IT services that facilitate and enhance teaching, learning and administration in the School community. This policy provides guidance so that staff, students and other authorised users can access the School's IT resources safely, securely and within the law, and so that girls are educated to use email, internet, mobile phones and social media appropriately. It applies to the use of School IT resources, whether on or off School premises, including laptops and mobile computing devices, software, operating systems, storage media and network accounts that provide access to local network, internet and email resources.

Responsibilities

The IT department aim to safeguard IT resources and the integrity of data stored on them, minimise the liability arising from the misuse of IT resources and data and ensure that the confidentiality of data is protected to the extent allowed or required by all laws pertaining to it. They ensure that all users have use of resources allocated to them from any networked computer in accordance with their role, so they are able to access the network in order to support and promote learning. Any deviation from this must be authorised by the Network Manager in accordance with the Data Protection Act 2018. The School monitors the network for any breaches of policy. This is recommended by Child Exploitation and Online Protection Centre (CEOP). Although all network traffic is monitored, only signs of misuse and abuse are logged and kept to be dealt with by the appropriate authority. When a breach of this policy is reported, it will initially be reviewed by the IT Manager and passed to the Deputy Head Pastoral for further review in accordance with the Behaviour Policy or Staff Disciplinary Procedures. Where a breach of this policy involves cyber bullying or sexting, it may constitute abuse, and thus the Safeguarding Children (Child Protection) Policy and Anti-bullying policies will also be referred to. Within the terms of the Data Protection Act 2018, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the School may record or inspect any information transmitted through or stored in its IT resources, including email communications, voicemail and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- The integrity, security or functionality of IT resources, or the liability of the School needs protecting.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the IT facilities.
- Investigating or detecting unauthorised use of IT facilities and preventing or detecting crime.
- Ensuring effective operation of IT facilities.
- Determining if communications are relevant to the business (for example, in the last resort where a staff member is off sick or on holiday and business continuity is threatened).
- It is otherwise permitted or required by law.

All users of Queenwood's IT resources must:

- Read and understand this policy, comply with all laws pertaining to their access, including copyright, libel, fraud, discrimination and obscenity laws.
- Abide by this policy and all policies and laws relating to the use of IT, act in a responsible, lawful and ethical manner and be aware that some data including email and documents stored on the system may be accessible under the Data Protection Act 2018.
- Not share their password but if necessary change their password.
- Never use another user's account or attempt to access another user account.
- Never access another user's personal electronic documents (email included) without the owner's express permission or as allowed by law.
- Ensure that no computer allocated to them is left insecure. This is particularly important for staff.

No person may knowingly:

- Copy, save or redistribute copyright-protected material without approval, (eg music and videos);
- Connect a device to the network or any IT resource without prior approval, this includes VOIP phones, laptops, PDAs, Gaming devices, mobile phones etc;
- Use the network in such a way that the use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- Create, transmit, retrieve, send, copy or display offensive, pornographic, obscene, defamatory or racist messages or pictures;
- Damage computers, computer systems or computer networks or install programs without approval;
- Use another user's account and/or attempt to obtain their password;
- Corrupt or destroy other user's data or disrupt the work of other users;
- Introduce or attempt to introduce a virus or malicious software;
- Attempt to bypass network or computer security including Antivirus Software, using programmable scripts or network monitoring software or any other method;
- Attempt to gain access to or use resources not allocated to them;
- Use illegal Peer to Peer file sharing programs;
- Use externally based email for School purposes (staff only), as this is potentially insecure and could breach the Data Protection Act 2018 or the Children Act 2004.
- Record, film or take photos without permission on a trip or at school. Queenswood reserves the right to use photographs of students for marketing purposes unless parents have opted out. In the parent contract parents are asked to contact the Principal in writing if they do not wish to have photographs of their daughter used in promotional material. In addition all users must ensure that the use of any words and photographic images should be appropriate and not perceived to be harmful to a girl or member of staff in any way.
- Encourage radicalisation.
- At School events, including drama and dance performances, concerts and sporting events, parents, visitors and girls will be reminded in programmes of the following:

Drama/Dance

The use of cameras and recording devices is prohibited during the performance. Pictures and videos may be taken at the end of the show of your daughter/ward only.

Music

Please note that the use of cameras and recording devices must be restricted to your daughter/ward's performance only.

Sport

Please note that the use of cameras and recording devices must be restricted to your daughter/ward's event only.

Users should inform the Network Manager if they believe that attempts have been made to use the network or internet in an unacceptable manner or if they discover any materials they consider to be offensive or inappropriate.

All users must comply with the provisions of the Acts of Parliament in Appendix 1 and with Appendices 2 - 5 of this Policy.

Other related school policies and procedures

- Pupil version of policy in Boarding Houses
- Aims and Ethos
- Anti-Bullying Policy
- Behaviour Policy
- Safeguarding Children (Child Protection) Policy
- Expulsion Removal and Review Policy
- Staff Employment Handbook
- School Policy on Conduct found in the Employment Handbook
- Conducting a Search Policy

APPENDIX 1 APPLICABLE ACTS OF PARLIAMENT

Computer Misuse Act 1990: This Act makes it an offence to erase or amend data or programs without authority, obtain unauthorised access to a computer, "eavesdrop" on a computer, make unauthorised use of computer time or facilities, maliciously corrupt or erase data or programs or deny access to authorised users.

Copyright, Designs and Patents Act 1988: This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sounds, moving images, TV broadcasts and many other media.

Crime & Disorder Act 1998: The Crime and Disorder Act provides the requirement for partnerships between the police, probation, local authorities, health authorities and other agencies. This includes locally targeted and data based strategies that are agreed with the communities. It is important to note that the Crime and Disorder Act 1998, for the first time placed the coordination of community safety and crime prevention on a statutory basis. Section 5 of the Act makes local authorities and chief police officers the 'responsible authorities' for setting and implementing strategies aimed at achieving reductions in crime.

Data Protection Act 2018: This has replaced the 1998 Act and implemented the provisions of the EU General Data Protection Regulation.

Privacy and Electronic Communications (EC Directive) Regulations 2003: This new directive extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial email (UCE or Spam) and SMS to mobile telephones; UCE and SMS will be subject to a prior consent requirement, so the receiver is required to agree to it in advance, except in the context of an existing customer relationship, where companies may continue to market their own similar products on an 'opt-out' basis.

Protection from Harassment Act 1997: A person must not pursue a course of conduct which he/she knows or ought to know amounts to harassment of the other. For the purposes of this section, the person whose course of conduct is in question ought to know that it amounts to harassment of another if a reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other. Subsection (1) does not apply to a course of conduct if the person who pursued it shows: that it was pursued for the purpose of preventing or detecting crime, that it was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or that in the particular circumstances the pursuit of the course of conduct was reasonable.

Protection of Children Act 1978, as amended by Sect 84 of the Criminal Justice and Public Order Act 1994

Children Act 1989 and 2004

Malicious Communications Act 1988: This includes harassment, bullying, and cyber-stalking.

Sexual Offences Act 2003: Having and distributing indecent images is an offence, and encouraging or inciting someone to take or send 'sexts' may be illegal.

The Obscene Publications Act 1959 and 1964: This includes illegal material on, or transmitted via, the web and electronic communications.

The Communications Act 2003: This includes illegal material on, or transmitted via, the web and electronic communications.

APPENDIX 2

EMAIL ACCEPTABLE USE POLICY

Introduction

Queenswood School ('Queenswood') provides and permits the use of electronic mail (email) within Queenswood. Queenswood encourages the use of email as an effective and reliable form of communication.

Users who have been granted the right to use Queenswood's email services are required to comply with this policy.

This policy must be read in conjunction with the Electronic and Social Media Policy.

Staff and students must take all reasonable measures to ensure that the content of any electronic communication is acceptable. All email must comply with current legislation and not create unnecessary risk to Queenswood.

This policy applies to the use of email on School premises and also any use, whether on or off School premises, which affects the welfare of other staff and students or where the culture or reputation of the School are put at risk.

Unacceptable behaviour

Queenswood accepts that the use of email is a valuable communication tool. Queenswood encourages appropriate and sensible use of email. However, it must be noted that emails are an official record of communication and may have legally binding consequences. Misuse of this facility can have a negative impact upon the business and the reputation of the School.

Unacceptable behaviour includes the following:

- reading other emails without consent;
- sending emails from other accounts without consent;
- use of Queenswood communications systems to set up personal businesses or send chain letters;
- forwarding of confidential messages to external locations;
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as bullying or harassment, or encourage radicalisation.
- accessing copyrighted information in a way that violates the copyright;
- breaking into Queenswood's or another organisation's system or unauthorised use of a password/mailbox;
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters including encouraging radicalisation;
- transmitting unsolicited commercial or advertising material;
- undertaking deliberate activities that waste networked resources;
- intentionally or negligently introducing any form of computer virus or malware into the Queenswood network.

Email and Queenswood students

When staff and students of Queenswood are communicating by email, this must be done through their respective Queenswood email accounts only, in accordance with the Data Protection Act 2018 or the Children Act 2004. Staff should not communicate with or befriend students of Queenswood through personal email accounts or any form of social networking media (e.g. Hotmail, Facebook).

Confiscation

Unacceptable use of electronic equipment could lead to confiscation in accordance with the School's Behaviour Policy.

Monitoring

Queenswood's email resources are provided for business and education purposes. Therefore, Queenswood maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, Queenswood uses monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with procedure.

Sanctions

Where it is believed that a student has failed to comply with this policy, they may be subject to the sanctions set out in the Behaviour Policy.

Where it is believed that a staff member has failed to comply with this policy, they may face disciplinary action, ranging from a verbal warning to dismissal, depending on factors such as the seriousness of the breach and the employee's disciplinary record.

Queenswood also reserves the right to withdraw or limit email access from anyone that may be in breach of this policy.

Legal proceedings

Users should be aware that emails can be disclosed as evidence in court proceedings and in response to data subject access requests made under the Data Protection Act 2018. Even if emails are deleted, a copy may exist on a back-up system or other storage area.

Agreement

Users who have been granted the right to use Queenswood's email services are required to comply with this policy.

APPENDIX 3

INTERNET ACCEPTABLE USE POLICY

Introduction

Queenswood School ('Queenswood') provides high speed cabled and wireless internet access for all staff and students. All internet access is subject to appropriate filtering and is monitored. Use of the internet is permitted and encouraged where such use supports the goals and objectives of the School. Use of the internet is primarily for work related purposes, however reasonable recreational browsing is permitted. Use of the internet must not interfere with any individual's responsibilities or the responsibilities any other member of the Queenswood community.

All company employees, volunteers, contractors or temporary staff who have been granted the right to use Queenswood's internet are required to comply with this policy.

Internet access is available on all computers on the Queenswood Network. This document should be read in conjunction with the Electronic and Social Media Policy.

Queenswood has a policy for the use of the internet whereby staff and students must ensure that they:

- comply with current legislation;
- use the internet in an acceptable way; and
- do not create unnecessary risk to themselves or Queenswood by their misuse of the internet.

Failure to comply with this policy will constitute a disciplinary offence and will be dealt with under the School's Disciplinary Procedure and would constitute gross misconduct. Internet access may be withdrawn without notice at the discretion of the Principal whilst allegations of unsuitable use are investigated by the School.

Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour:

- sharing of usernames and passwords;
- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material including any which encourage radicalisation;
- using the computer to perpetrate any form of fraud, or software, film or music piracy;
- using the internet to send offensive, abusive or harassing material to other users;
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- hacking into unauthorised areas;
- publishing defamatory and/or knowingly false material about Queenswood, your colleagues and/or any other member of the Queenswood community on any online publishing format including social networking sites;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of malicious software into the corporate network deliberately or negligently;
- intentionally trying to bypass Queenswood filtering systems;

- use of illegal file sharing/peer to peer systems;
- use of the internet to enter into any contract or subscription on behalf the School, without specific permission from the Principal or a member of staff to whom she has delegated this authority.

Internet access may be withdrawn without notice at the discretion of the Principal whilst allegations of unsuitable use are investigated by the School.

School-owned information held on third-party websites

If school-related information is produced or collected, the information remains the property of Queenswood. This includes such information stored on third-party websites such as web mail service providers and social networking sites.

Student and Staff online interaction

Electronic communication between staff and students may only occur between their respective Queenswood email accounts. Staff should not communicate with students or students with staff through personal email accounts or any form of social networking media (e.g. Facebook, Twitter, Snapchat).

Monitoring

Misuse of the internet can have a negative impact upon the business and the reputation of the School.

Queenswood monitors and filters the internet according to policies set by the IT Department in accordance with this policy and any applicable laws. No attempt must be made to bypass the filtering system.

Sanctions

Where it is believed that a student has failed to comply with this policy, appropriate measures will be taken in accordance with the Behaviour Policy.

Where it is believed that a staff member has failed to comply with this policy, they may face disciplinary action. If the staff member is found to have breached the policy, they may face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

Queenswood also reserves the right to limit or withdraw internet access to anyone if it is believed or suspected that this policy has been breached.

Agreement

All School employees, volunteers, contractors or temporary staff who have been granted the right to use Queenswood's internet are required to comply with this policy.

APPENDIX 4

ACCEPTABLE USE OF MOBILE PHONES BY GIRLS POLICY

AIM

To guide the girls towards the appropriate and acceptable use of technology and in particular, handheld devices.

GUIDELINES

- Where appropriate, the use of technology to support learning is strongly encouraged.
- Girls should have only one phone in school.
- Mobile phone numbers must be registered with their House staff.
- Girls are advised not to keep phones with them during the school day as they can be stored safely in the House or lockers during lesson time. However, phones, tablets, laptops etc may be used in lessons, with teacher permission and under guidance.
- Misuse or inappropriate use of any device will lead to confiscation. Further sanctions may be applied if the aforementioned use causes embarrassment or discomfort to someone else.

ACCEPTABLE USE

- Mobile phones may be used in House or the Sixth Form Centre during the working day (08:20 to 18:00). They should not be taken to activities.
- All Year 7 pupils must leave their phones in Stamp at all times. They may only be used with the permission of house staff. Boarders will have dedicated times that they may use their phones.
- All mobile devices should be switched off and kept out of sight during lessons, tutorial, co-curricular activities, in the queue for meals, outside classrooms and when moving between buildings on the school site. The only exception to this is if permission has been given by a member of staff e.g. in a lesson.
- We recognise the importance of emerging technology and that teachers may wish to use the function of a mobile phone/tablet, such as the camera, to aid teaching. On these occasions, girls may use their device in the classroom if the member of staff has given permission. This does not apply to Year 7 who do not have access to their devices.
- All devices will be collected in at night from Years 7, 8 and 9.
- No device may be used in the Dining Room at any time by girls or staff or in the queue for meals.
- Parents/guardians are reminded that in the case of an emergency, they should contact the General Office (8am – 6pm) or their daughter's Housemistress/Houseparent to ensure a girl is reached quickly and assisted in an appropriate way.
- Filming, texting and loading of material onto or down from the Internet must be appropriate.

INAPPROPRIATE USE

This is defined by the use of a mobile device causing disruption and/or discomfort/embarrassment to fellow pupils, staff or member of society.
It is strictly forbidden to take photographs or videos that will humiliate a pupil/staff member and then send them to other pupils or upload to the Internet.
It is a criminal offence to use a mobile phone to harass or offend another person. Calls, text messages, WhatsApp messages, Snapchat, etc and emails can be traced from all devices.

SANCTIONS FOR INAPPROPRIATE USE

- First offence: the device will be confiscated and put in the relevant Housemistress/Houseparent's pigeon hole. It will then be returned to the pupil at the end of the *following* day – 18:00 (or 16:20 if leaving school at this time). This will be recorded by the Housemistress/Houseparent as a sanction on iSAMS. Parent/ guardian will also be contacted by the House staff.
- Second Offence: the device will be confiscated and put in the relevant Housemistress/Houseparent's pigeon hole. It will then be returned to the pupil at the end of the second working day following confiscation– i.e. a minimum of 48 hours' later. The Head of Section will be informed and the sanction will be recorded on iSAMS by the Housemistress/Houseparent. The parent/ guardian will be contacted by the Head of Section.
- Third offence: the device will be confiscated and put in the relevant Housemistress/Houseparent's pigeon hole. The parent/ guardian will be contacted by the Deputy Head Pastoral and the pupil's right to have a mobile phone/smart phone in school will be reviewed. The device will be returned following the outcome of this review which is likely to be a minimum of seven days. This sanction will be recorded on iSAMS by the Deputy Head Pastoral and the pupil will sit a Deputy Head's detention.
- Further sanctions may be applied if the use causes embarrassment or discomfort to someone else. Girls may face disciplinary action as sanctioned by the Principal or Deputy Head Pastoral.

THEFT OR DAMAGE

- Girls should name their devices clearly on the cover.
- All devices should be locked away at school or handed in to House staff.
- The school accepts no responsibility for replacing lost, stolen or damaged devices.
- It is strongly advised that girls use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phone and that all devices are kept secure.

ROLES AND RESPONSIBILITIES

- The school makes it clear to parents and girls that all mobile devices are the responsibility of the girls.
- Girls have a responsibility to use their devices, especially phones, at appropriate times and in sensible ways.
- Staff have a responsibility to enforce this acceptable use and lead by example.
- If a member of staff confiscates a technological device, then they must make sure that it is given to the relevant Housemistress/Houseparent or to the Deputy Head Pastoral.
- The Deputy Head Pastoral has the responsibility of reviewing the policy and practice on an annual basis.

PRACTICE

- The school writes to parents annually to remind them about the mobile phone policy and appropriate use of all mobile devices. Parents are asked to discuss these guidelines with their daughters.
- Girls are reminded frequently about the appropriate use of their devices.
- The response as outlined by the Rewards and Sanctions policy is carried out by staff.
- If a girl's phone is confiscated, then it must be made clear that she has access to other school phones and may still communicate with her parents/guardian. Every girl has access to a phone in their House. They must ask permission before use.

APPENDIX 5

ACCEPTABLE USE OF SOCIAL MEDIA

Introduction

This Policy covers any device used for storing data and online sites where messages or files can be posted, including but not limited to USB memory sticks, memory cards, CD/DVD/Blu-Ray discs, external hard drives, Facebook, MySpace, Flickr, Twitter, Bebo, RateMyTeacher etc. Queenswood encourages the acceptable use of social media sites by pupils and acknowledges its place in increasing opportunities to learn and in promoting positive, respectful and thought-provoking discussions. Narratives posted onto social-media sites have the potential for considerable breadth of dissemination and individuals choosing to post onto such sites should be mindful of this. Queenswood therefore expects that discussions pupils and staff participate in are polite and non-offensive.

Acceptable use

When posting material onto social media sites pupils and staff should be conscious of the need to keep their school/professional life and personal life separate. There is a catch-all offence under Section 127 of the Communications Act 2003. This makes it illegal to send "by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character".

As such, pupils and staff must not:

- Put themselves into a position where anything posted might bring Queenswood into disrepute.
- Represent their own personal views as those of Queenswood on any social media sites.
- Post any narrative that could be considered either implicitly or explicitly as insulting, threatening, harassing, illegal, abusive, obscene, defamatory, slanderous, or hostile towards any individual or Queenswood, in keeping with the Anti-Bullying Policy.
- Discuss or post personal information about other pupils or members of staff at Queenswood including phone numbers, email addresses or any confidential information.
- Post any material that compromises the rights of any Queenswood pupil or member of staff of any Queenswood entity, including privacy, intellectual property or publication rights.
- Allow any other individual or entity to use your identification for posting or viewing comments.
- Post comments under multiple names or using another person's name.
- Encourage radicalisation or post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views or encouraging others to do so.
- Breach the provisions of applicable data protection laws.

Staff should not set tasks which involve uploading on to social media. Tasks may still be set which reflect that style.

All information posted onto a Queenswood-sponsored social media site or any 'open' social media site will be publicly available on the Internet. This information will not be subject to any additional privacy or protection. All members of the School community using any social media site should be aware that their name may appear next to any information posted and could be linked and traced

accordingly. Comments posted which contravene this policy may be subject to disciplinary action and sanctions outlined below.

All material posted onto a Queenswood-sponsored social media site becomes the property of Queenswood. Individuals posting comments or materials here lose all subsequent rights to this material which may be disseminated by the School in whatever way it decides. Queenswood reserves the right to delete comments from social media sites and will take all reasonable steps to have offensive material removed from websites on behalf of their pupils, staff or in order to preserve the reputation of the School.

Sanctions for Pupils

The full range of sanctions that are available to the School may be used in dealing with a breach of this policy in keeping with Queenswood's other policies. The specific disciplinary sanction imposed will depend on the seriousness of the incident and will be more severe for repeated offences and may include:

- A verbal reprimand/warning for those involved naively or unwittingly at a low level.
- Prohibition from using the Internet or other ICT for a period of time.
- Confiscation of mobile devices: schools have the power to confiscate phones.
- Periods of detention, either during the School week or at the weekend.
- Suspension/expulsion, irrespective of the pupil's school record.

The School reserves the right to report infringements of this policy to the Police when it considers that a criminal offence (such as harassment, abuse, racism) has been committed.

Staff

Queenswood is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the School are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- common law and an employee's duty of confidentiality, and
- the Data Protection Act 2018.

Confidential information includes, but is not limited to person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 2018 and information divulged in the expectation of confidentiality.

Staff should not be 'Friends' or 'Followers' of pupils, or connect with pupils on any social media network. It would be considered inappropriate to connect with pupils on a personal account. It may in some circumstances be inappropriate to connect with parents, guardians or carers. The School recommends the highest privacy settings on all social media accounts. Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- Protection from Harassment Act 1997

- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1988
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

Queenswood could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render Queenswood liable to the injured party.

Sanctions

Failure to comply with this policy will constitute a disciplinary offence and will be dealt with under the School's Disciplinary Procedure and would constitute gross misconduct. Internet access may be withdrawn without notice at the discretion of the Principal whilst allegations of unsuitable use are investigated by the School.