Queensgate Foundation Primary School

Internet and email acceptable use Policy
FEBRUARY 2016

Internet and Email acceptable use Policy
Queensgate Foundation Primary School

Policy Review

This policy was adopted by the Full Governing Body on 25th February 2016 and will be reviewed on a regular basis.

The policy was last reviewed and agreed by the Governing Body on 25th February 2016

It is due for review Spring 2020 (up to 48 months from the above date).

Signature ...*Sillito*... Head Teacher   Date *26th March 2016*,

Signature ...*M. J. Lloyd*... Chair of Governors   Date *21-03-16*.

Working together for a successful future

References

Introduction The internet and e-mail are now indispensable tools for all school teaching staff, managers and administrators. While they offer huge potential benefits to improving work efficiency and effectiveness if properly applied, they also pose significant risks for the school.

This acceptable use policy, provides staff/governors/pupils/visitors at Queensgate with guidance on how to make best use of these technologies whilst understanding the potential dangers.

Pupils

Pupil Use of the School's Internet and E-mail Services

The following is a series of statements indicating how pupils should use internet and e-mail services at the school.

- Ensure that you are aware of the relevant internet and e-mail based skills that you are teaching the pupils
- Use focused search tasks rather than very open research tasks for younger pupils to ensure that accidental access to inappropriate web sites is reduced
- Use sites saved to favourites whenever possible to reduce accidental access to other sites. Use sites know to be child safe whenever possible
- Check any open searches you intend to ask pupils to do in advance to ensure you are aware of the risks. Minimise the opportunities for any misspellings by the children as misspellings may cause inappropriate material to be found
- Ensure you know the procedure to follow if a pupil finds an unsafe site during lesson time. The suggested procedure would be to remove the screen from the children's view, either by turning off the monitor or, in the case of laptops, closing the lid. In either case, leave the computer on so that you can make a note of the web address. Report this to the ICT Coordinator straight away so that future access can be prevented
- Teach pupils what to do if they accidentally find an unsafe site while using the internet
- Teach pupils not to use any personal information such as name or address at any time when e-mailing or using the internet (e.g. at home or school) and the reasons why this could be unsafe. Teach pupils to involve teachers, parents and carers whenever they are communicating with people they do not know
- Teach pupils to use the internet responsibly and to speak to their teacher, parents or carers if they feel unsure or unsafe
- Teach pupils that web sources could be unreliable and inaccurate and to check their information against other sources and not to rely on just one information source
- Supervise pupil use of the internet and e-mail
- Ensure parents are made aware of the risks of internet and e-mail use in order that they can take precautions at home
- Be aware that searches for images may result in unsafe images as pictures are not easy to filter out. Test the search first and check not just the first page/s of returns to be sure
- Younger pupils will not be able to use the internet unsupervised
- Don't let staff use the internet or e-mail with pupils who are not familiar with this Acceptable Use Policy

Staff and supply teachers

School Web Sites and Use of Images

- The most serious risk to pupils using the internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being disclosed online. Pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm. The risk to children may not be immediate, since there can be a long period of building up a relationship, known as the 'grooming process'
- On no account should either first names or surnames be attached to photos of children on websites. Care must be exercised that the filename of a photograph (e.g. janesmith.jpg) does not inadvertently identify a child.
- School websites should not include close-up pictures of children. All photographs of children should be general. Photos should be taken in such a way as to ensure that the individual identity of a child is protected (e.g. from an angle, in profile, at a distance.) If a website includes a child's photo, it could be downloaded from the web and edited in an unpleasant or embarrassing way
- Parental permission is sought at the start of the academic year to allow pictures or examples of pupils' work to be published on a website or other instances in the public domain. Where there are specific circumstances e.g. magazine or newspaper publication, permission will be confirmed on a case by case basis. Efforts should be made to ensure that parents understand the implications before giving permission.
- Ensure that no photographs are published in a way which makes individuals identifiable, i.e. do not publish names or other labels with photographs where pupils may be recognised
- Press coverage is encouraged where this builds confidence, pupil esteem or positive images in the community but the school, staff, pupils and children are reminded they have a right to say no if it is not in the best interests of the school or the individual or will breach privacy
- Guidelines for taking photographs are made clear to parents at events which enable parents to opt out if they wish and not have their child included
- Ensure consent is gained in advance for any events to which the press are invited to photograph individuals
- Refuse to allow images to be taken by journalists/others who attend a school without invitation
- Do not include a child's photograph on a web page where the child's name has been used. This also applies to media coverage and head teachers are within their rights to not give pupil full names or personal information to go with photographs of pupils.
- Do not sign blanket consent forms from media companies; instead insist on specific details of photographs being taken and used

Staff Use of the School's Internet Service

- The school wishes to encourage the use of e-mail and internet by staff in support of their work. Whilst staff are encouraged to use e-mail and the internet in support of their work all use of these facilities should be appropriate to the work, standards and ethos of the school

- The use of the school's internet and e-mail systems is not provided as a right to any of their users. They may be withdrawn from any user, who does not conform to this Acceptable Use Policy
- The school is responsible for authorising any user of its internet or e-mail facilities, and should monitor and police their use
- Any member of staff who commits a serious offence in the use of the schools internet service may be subject to the school's staff disciplinary procedures.
- Illegal activity using the school's internet service will be reported to the police as necessary
- Staff should not use the school's e-mail and internet system for personal use during school time, except where specifically authorised by senior school management.
- Never pass on, make obvious or leave in an insecure place any passwords associated with using the internet, e-mail and computer system
- Goods and services may be ordered directly via the internet as per the school's procurement procedures
- Never provide personal details or contact details of your own, or any other person, to internet sites including weblogs, forums or chat rooms. Exceptions should be checked with your line manager or Headteacher. At all times comply with the Data Protection Act
- If you see any unacceptable site or material as a result of an innocent internet query, unsolicited pop-up window or in any other way, report it immediately to the headteacher, the IT subject leader or IT technician. Action can then be taken to block the site or material
- Staff or approved adult school users should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet
- Staff using a school Laptop or other device off the school site, at home or elsewhere, will still have to abide by the school internet Acceptable Use Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the Computer Misuse Act (1990)
- Never upload an image to a web site without complying with the School's guidance on images loaded to the internet
- Staff will at all times work to maximise the safety of pupils within their care in their use of the internet
- Colleagues will be aware of the ethos, standards, equalities and ethnic mix of the school and will not access any internet material, or work with the internet, in any way that infringes or offends these
- This Acceptable internet Use Policy is for all school staff and approved adult users of the school, and will be posted, and/or made available, on the school website and under Policies in the Staff Share on the server

Behaviour and Discipline in Internet and E-mail Usage

While the school's general policy on behaviour can be found in the policy document Behaviour and Discipline, the policy with respect to online or cyber bullying is described below.

- Pupils should be made aware of the existence of online bullying

- Pupils should be made aware that if they feel they are the victim of online bullying they should approach a carer or a member of staff to let them know
- The school should regularly advise parents and guardians about the importance of esafety, making information available through accessible channels such as newsletters and the school website

Staff Use of the School's E-mail Service

E-mail Acceptable Use Statements

- Check your e-mail regularly - ignoring messages is discourteous and confusing to a sender
- Treat the content of any e-mail or an attachment that you prepare in the same way as any other paper based letter or document from a legal point of view. The Laws of the land apply equally to electronic messages and documents as they do to paper documents, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination. The content of the e-mail or an attachment must never infringe the law of the land and if sent from school should be in accordance with the values and ethos of the school. Remember it is easy for your e-mail to be passed on electronically to others should any recipient decide to do so
- Make sure your e-mail address is included on any contact information put onto paper-based letters or documents
- Remember that sending an e-mail from your school e-mail account is similar to sending a letter on school letter headed paper. Do not in any way bring discredit or embarrassment to the school or local authority
- Any e-mail received by a member of staff, which is regarded as illegal or offensive, should be reported to the Headteacher immediately. Similarly, any e-mail received by a student, which is regarded as illegal or offensive, should be reported to the Headteacher immediately
- To safeguard against computer viruses do not open external e-mails or an e-mail attachment that look in any way suspicious. Report it to your school's ICT co-ordinator for checking
- Do not make changes to someone else's e-mail and then pass it on without making it clear where you have made the changes. Not to do this is a form of misrepresentation
- Do not copy images or any other material for use in your e-mail or an attachment that infringe the copyright law
- Do not, under any circumstances, give your Portal / e-mail password to anyone else.
- Do not print out all your e-mail messages as a matter of course. Only print those for which it is an absolute necessity to do so
- Do not broadcast an e-mail to any group of recipients unless it is necessary. It is very easy to do, but can be very annoying to recipients and wastes resources
- Unless you are authorised to do so, do not send an e-mail to any supplier that could be interpreted as creating a contract in any way. In general, do not use e-mails for contractual purposes. NOTE: Within the law, a user could send an e-mail contain wording which may form a legally binding contract with a supplier
- Do not attempt to read another person's e-mail

- Staff use of school laptops or other items of IT equipment at home (or in school but out of school hours) to access the internet and e-mails must conform to the expectations above

Social Contact and Social Networking

- Social networking sites and blogging are extremely popular. Staff/governors must not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct
- Staff/governors in school should not establish or seek to establish social contact with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship. This includes social networking sites such as Twitter, Facebook, Snapchat, Instagram and blogging. Even if a pupil seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise her/his professional judgment in making a response and be aware that such social contact in person, by phone or on the internet could be misconstrued and may place the member of staff in a very vulnerable position
- Staff/governors must never give their personal details such as home/mobile phone number, home or e-mail address. The school e-mail system or a school phone should be used instead