Internet Access and Acceptable Use Policies

The school's e-Safety Officer is Mr M Johnson.

Internet access is very widely available throughout the school. When using computers and the Internet we ask pupils and staff to follow the appropriate acceptable use policies.

Each pupil will be required to agree to an appropriate acceptable use policy which will be done via our school intranet. The policy may change during the course of the year and in which case students and staff would be expected to agree to this new policy. Access to our intranet is restricted until the policy has been electronically signed.

This is accepted standard practice in all work places where people have access to and use computers.

General

- On their first lesson the AUP will be explained to Y7.
- Food and drink must not be consumed near the computers

Sanctions

- If Y12/13 students are caught breaking the AUP then staff should report the student to Miss Allen (who will liaise with the E-Safety Officer) by email. The student will have certain network privileges revoked for a specified time, depending on the nature of the infringement. If there is a second offence, parental contact will be made and certain network privileges will be revoked.
- If a Y7-11 student is caught breaking the AUP, staff should report the student to the Head of School through the online behaviour sanctions system and a school recorded detention will usually be issued. If any student is caught for a second time, the Head of School will contact parents and certain network privileges will be revoked for a minimum of a two week period.
- If a student is reported for a third time then Miss Francis is to be directly involved and a fixed term exclusion will be considered.
- NB At any stage an exclusion is likely if inappropriate/pornographic images are being accessed.

Reviewed June 2015

ICT Acceptable Use Policy: all pupils attending QEGS, Alford

I understand that using the computer network is a privilege and that when using the school computers I will:

- always behave in a sensible, mature way, respecting others at all times
- only log on using my own username and keep my password secret
- report any suspected breach of network security (whether by myself or others) to a member of staff
- refrain from accessing any newsgroups, links, web pages or other areas of cyberspace that would be considered offensive because of pornographic, racist, violent, illegal or illicit content
- never use my school email address to sign up to social networking sites such as Facebook
- take responsibility for monitoring and appropriately rejecting any such newsgroups, links, web pages or other areas of cyberspace accessed by me
- only use the school computer network for school-related work
- always be courteous and use appropriate language both to those around me and those I contact through the network
- never seek to harass or abuse fellow students or members of staff through the use of obscene or offensive language or images, either on the school network itself or via external social networking sites, and will report any cases of such usage against me
- not allow copyrighted material to enter the school eg MP3 files
- not download software, games, music, graphics or video without first checking copyright and asking my teacher
- use any downloaded material in an appropriate manner in my work, listing its source in a bibliography and clearly specifying any directly quoted material
- never reveal personal information including names, addresses, credit card details, telephone or fax numbers and photographs of myself or others
- never subscribe to auto-mailing systems
- only use the academy address where I have permission and will never give other details about the academy, including telephone numbers
- not interfere with or damage the school computers or peripherals, the school systems or network in any way
- report any accidental damage immediately to a member of staff
- report any misuse of the Internet or email to a member of staff
- not use any systems outside of the academy in a way which could cause offence either to staff or to other pupils at the academy
- not use any systems outside of the academy in a way in which could portray the academy in a negative way
- not try to add members of staff as “friends” on social networking sites
- report any instances of others breaching any of the points above

I understand that my school account is not, and cannot be, regarded as private and will be subject to random monitoring. I understand that if I am found not to be complying with this policy I will be denied access to the computer network for a time to be determined by my head of school in liaison with the academy’s e-safety officer. I also understand that I may face further disciplinary action depending on the nature of the offence.

Reviewed June 2015

ICT Acceptable Use Policy for all adults working at QEGS, Alford

All adults using ICT equipment within the academy must ensure that they have read and abide by the Acceptable Use Policy. If they are found to have contravened any of the requirements they may face disciplinary action.

The academy's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes but **occasional** personal use is permitted. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

When using ICT equipment I will not

- give anyone access to my login name or password (unless authorised by the Headteacher)
- attempt to introduce any unlicensed applications
- corrupt, interfere with or destroy any other user's information
- release any personal details of any colleague or pupil over the Internet
- use the school internet access for business, profit, advertising or political purposes
- leave my account open at the end of a session
- engage in any activity which might compromise the security of the school network
- connect personal equipment to the academy's network without seeking permission from the ICT Systems Manager. Individuals should be aware where personal equipment is connected to the network certain information about their equipment will be logged.
- use personal equipment that does not have the suitable virus protection software. It is the responsibility of the owner to ensure that this is the case but help can be sought from the ICT Technical Team.

When using e-mail I will

- observe 'netiquette' on all occasions. E-mail should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny.
- not include offensive or abusive language in my messages nor any language which could be considered defamatory, obscene, menacing or illegal
- not use language that could be calculated to incite hatred against any ethnic, religious or other minority
- make sure that nothing in messages could be interpreted as libellous
- not send any message which is likely to cause annoyance, inconvenience or needless anxiety
- not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes
- only use the school email system when communicating with pupils and not any private methods of communication.

When using the Internet I will

- watch for accidental access to inappropriate materials and report any offending site so that action can be taken
- check copyright before publishing any work and ensure that any necessary permissions are obtained
- ensure that the academy's photo policy is strictly adhered to
- report any breaches of the Internet policy

When using outside systems I will

- make sure that any information I share on social networking sites takes into account my role as a member of staff
- not allow pupils to be “friends” with me on social networking sites

To protect the data of students and staff I will

- only access data on students and staff through the school supplied MIS, Integris or the school Intranet
- keep all data I store about students and staff safe.
    - In a paper form this needs to be in a locked filing cabinet or in electronic form needs to have password/encryption
- not keep any personal details of students such as address, telephone numbers in a document, electronic form that is not kept safe
- not keep any personal details about colleagues such as address, telephone numbers in document, electronic form that is not kept safe
    - Obvious exceptions such as phone numbers for personal use is outside this scope
- never send personal details about staff or students to organisations/people outside of Queen Elizabeth’s unless the data is a necessary return from an approved external organisation.
    - These will generally done by reception, ICT or the Headteacher
- ensure that any data I do hold about students is deleted/shredded when no longer needed
- report any theft of any electronic device containing student data or paper copies as soon as possible
- remove any data from a personal device that may have links to students before I sell the device
    - If the device is school owned then this will be done by ICT
- never leave personal details about students/staff in a public place and unattended
- never ask a student for personal information unless the need has been agreed by the headteacher
- ensure any data that is passed to me to be updated is given to the school office for processing
- ask for clarification from the ICT Systems Manager/Headteacher if I am sure about whether I am contravening the Data Protection Act.

Revised June 2015