Queen Elizabeth's Grammar, Alford
A Selective Academy

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

At Queen Elizabeth's Grammar, Alford the named persons with responsibility for this Policy are:

Authors	Mr G Thompson & Mr M Johnson
Governor	Full Governing Body

Approved by: Policies Committee
Date Approved: 6 June 2022
Last reviewed: 6 June 2022
Next date due to be reviewed by the Governors: June 2025

1

Queen Elizabeth's Grammar, Alford
A Selective Academy

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 put anything about a pupil or colleague in an email (or on the intranet) that I would not be happy being seen by them. If they make a subject access request then I am aware that we have to supply this information.
- 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 parents and not any private methods of communication.
- if the email contains personal data about staff, students or parents, use the encryption method of adding QEGSENC in the subject line when sending material outside of the school

Queen Elizabeth's Grammar, Alford
A Selective Academy

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
- 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. Think carefully before posting information about our school – even if your account is private. Comments could be taken out of context and be damaging. Remember that it is an implicit condition of employment that an employee owes a duty of loyalty to an employer.
- ensure that if I have staff or student data on my personal computer or laptop, then I will password protect and nobody else in my family will know my password. If I feel that this is not possible then I will let ICT Systems Manager know and he will purchase some encrypted memory sticks for my use. I will try to keep as little student and staff data on my personal computers as possible, and store things on my h drive at school rather than the hard drive at home.
- not allow pupils to be "friends" with me on social networking sites

When using the school Intranet I will
- be mindful that all information I add about students could be read by parents if they request to under the General Data Protection Regulations (GDPR)

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
- 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 (unless for personal use)
- 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.   NB These will generally done by reception, ICT dept. or the Headteacher and his PA
- ensure that any data I do hold about students is deleted/shredded when no longer needed
- ensure that the academy's photo policy is strictly adhered to and will not keep photos of pupils on my mobile phone. Following a trip or event, I will forward some photos to the Headteacher for use in the Tuesday letter and other publications, then delete all photos from my phone.
- 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
- 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
- never transport student data on an unencrypted device between home and school (encrypted memory sticks can be purchased via the school if required)
- never leave school paperwork inside my car overnight
- not leave mark books or other documents with student data in classrooms unless they are stored in a locked filing cabinet or drawer.
- report any breaches of personal data involving students, staff or parents to the school's Data Protection Officer (Assistant Headteacher Curriculum & Standards).
- report any concerns about data protection to either the Headteacher, Data Protection Officer or ICT Systems Manager
- follow the school's retention policy for storing personal data and ensure that I delete the necessary files from areas where I have responsibility (i.e. H drive, departmental folders) as well as shred (at school in the reprographics office) any relevant documents.
- lock offices when not in use
- not put telephone numbers or personal details about pupils, staff or parents in emails. Integris should be used to access this information
- not write down details about pupils, staff or parents for my own use
- ask for clarification from the ICT Systems Manager/Headteacher if I am unsure about whether I am contravening the General Data Protection Regulations.

Approved by: Policies Committee
Date Approved: 6 June 2022
Last reviewed: 6 June 2022
Next date due to be reviewed by the Governors: June 2025

4