Quality First Education Trust

ICT Acceptable Use Policy
(code of conduct)

Approved by Board of Trustees on: 26 April 2018
Policy in effect from: **25 May 2018**
Date of next scheduled review: May 2020

It is everyone's duty to use ICT safely and responsibly. This is part of keeping children safe in our schools as well as ensuring we are compliant with the General Data Protection Regulation (GPDR). This policy (in the form of a code of conduct) should be read, understood and agreed by all **staff, local governors and trustees** within the Quality First Education Trust and its schools, and any visitors with relevant ICT access.

In the context of this policy, ICT covers all equipment (including mobile phones, digital cameras, laptops and tablets) and systems (e.g. the school and Trust IT systems, servers, internet, intranet and email) used in school or for school/Trust business. This policy also refers to use of ICT outside school business, where the reputation of the school or Trust may be affected. If you are not clear about whether something is or is not covered by this policy, you should speak to the headteacher.

This policy refers to other key policies. You should be aware of, and know where to find, the Q1E Data Protection Policy, Q1E Child Protection and Safeguarding Policy, and Q1E Online Safety Policy.

Remember

- You are responsible for all activity carried out under your username.
- If you are not sure about whether something is ok - it is your responsibility to check.

Reporting concerns

- You must report any incidents of concern regarding staff use of ICT and/or children's safety to a designated member of staff, in line with the Child Protection and Safeguarding Policy.

- You must report any potential data breach as soon as possible to the **Data Protection Officer (DPO).** This includes:
    - If you think that equipment containing non-encrypted personal data has been stolen or lost
    - If you think that a third party system containing personal data has been hacked (e.g. cashless payment provider or school information management system)
    - If you think that someone else has obtained your username/password details for school equipment, systems or email accounts
    - If you accidentally email or pass any personal data to an unauthorised individual (you should attempt to recall the email as soon as you become aware of the error)
    - If you receive personal data sent in error.

Use of school systems

- Make sure your passwords are strong, never share them and don't write them down.
- You should not use school/Trust ICT equipment or systems for non-school/Trust activities. It is a disciplinary offence to use school ICT equipment for any purpose not permitted by its owner.

- When using school equipment or accessing school servers you will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Internet use can be monitored and traced to individuals. Your internet use may be monitored and if anything untoward is uncovered, this could be logged and used in line with disciplinary procedures.
- You must not install any hardware or software on any school owned device without the head's permission.

Use of personal devices, systems or email accounts

- You should not use your personal email account to contact parents and other outside agencies.
- You must never share private email addresses or social media details with pupils.
- As far as possible, you should avoid using personal devices in the context of school or Trust business. You should never store children's personal data on a personal device.
- You must never keep photos or videos of children on your phone or other personal device. If you do need to take a photo or video, you should ideally use a school camera. Use of personal devices for this purpose should be agreed in advance with the head, and in these cases photos or videos should be uploaded onto the school system as soon as possible, and deleted from the personal device

Looking after data

- You must take every precaution to ensure that data is kept secure and is used appropriately.
- When logged onto a PC, remember to 'lock' it when you step away from your desk.
- You must never use a USB stick (memory stick) or a personal email address to store or transfer unencrypted personal information about staff or children, exam results or any other sensitive data.
- You should avoid sending personal data, non-anonymised pupil data, exam results or staff pay information via email, unless this is encrypted, even within the Trust. Ideally staff should be able to find any information they need by logging into the relevant systems or files, therefore it is best to send a link rather than an attachment.
- You should not import children's personal data into any programmes not authorised by the headteacher, for example classroom management apps
- If you have hard (paper) copies of any sensitive information or personal data you must take care to keep it safe and secure, and destroy it appropriately once the school no longer needs it.

Using images and children's names

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use.
- In accordance with the Q1E Online Safety Policy, children's full names should not be used on a school website, blog, app or social media page, unless in exceptional circumstances when parental permission has been obtained (e.g. to celebrate an individual achievement in a news item).

Social media

- You should never contact, 'friend' or comment on post by a child on social networking sites or gaming platforms
- Always use social media carefully: check your privacy settings regularly, and think before you post or 'like' content which may bring your school into disrepute.

General

- You will make every effort to comply with copyright and intellectual property rights.