

ICT Acceptable Use Policy

(code of conduct)

Reviewed by Director of Operations and Data Protection Officer: March 2023

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 should be read, understood and agreed by all **staff, local governors and trustees** within the Quality First Education (Q1E) Trust and its schools, and any **visitors** **or volunteers** with relevant ICT access.

In the context of this policy, ICT covers all equipment (including mobile phones, cameras, laptops, tablets) and systems (e.g. school and trust IT systems, servers, internet, email) used in school or for school/trust business, and also use of ICT outside school/trust business, where the reputation of the school/Trust may be affected.

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** (which includes the safeguarding code of conduct, the safeguarding concern form and the neutral notification form), 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**

* Safeguarding: Report any concerns about children’s safety immediately, in line with the Q1E Child Protection and Safeguarding Policy.
* Neutral notification: Use the ‘neutral notification’ procedure to self-report any action you (or other adults) have taken which has the potential to be misconstrued or misinterpreted by others.
* Data protection: Report any data breach (or potential breach) as soon as possible to the trust’s **data protection lead** (charlotte.meade@q1e.org.uk), who will liaise with the data protection officer, e.g.:
	+ If you think equipment containing non-encrypted personal data has been stolen or lost;
	+ If you think a third party system containing personal data has been hacked (e.g. cashless payment provider or school information management system);
	+ If you think someone else has obtained your username/password details for school/trust ICT;
	+ 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. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (such as \* or %). Try incorporating three random words - easy to remember, hard to guess.
* Do 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.
* Do not install any hardware or software on a school owned device without the head’s permission.

**Use of personal devices, systems or email accounts**

* Do not use your personal email account to contact parents and other outside agencies.
* Never share private email addresses or social media details with pupils.
* As far as possible, avoid using personal devices in the context of school or Trust business.
* Never store children’s personal data on a personal device.
* 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**

* 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.
* Never use USB sticks to store or transfer unencrypted personal information about staff or children (including photos or videos), exam results or any other sensitive data.
* Avoid sending personal data, non-anonymised pupil data, exam results or staff pay information via email, unless encrypted, even within the Trust. Staff should be able to find any information they need by logging into the relevant systems or files, either within school or via remote access (via VPN connection to the network), therefore it is best to send a link rather than an attachment.
* Never use a personal email account to transfer school data/information.
* Never 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 keep it safe and secure, and destroy it appropriately once the school no longer needs it.

**Using images and children’s names**

* Images must 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, never use children’s full names 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**

* Never contact, ‘friend’ or comment on posts by a child on social networking 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.

**Remote** **learning, and working from home**

* When accessing personal data for remote learning/working, use the secure cloud access service.
* Conduct video sessions in a professional environment: correctly dressed, not in a room that is identifiable as a bedroom, and not having personal information or inappropriate objects in view.
* Behave towards pupils as you would in school - consider language, tone of voice and appearance.
* Do not start a remote lesson without another adult “in the room”.
* Do not arrange any online session without prior approval of the school, and never directly with a pupil.
* Do not use a personal system or personal login for remote teaching.
* Do not set up any IT system or platform on behalf of the school without SLT approval.
* Do not take secret recordings or screenshots of pupils or other adults.
* You may need to collect and/or share personal data, such as email addresses, to manage remote learning. As long as this processing is necessary for the school’s official functions, individuals won’t need to give permission. However, you must collect/share as little personal data as possible online.
* Take appropriate steps to ensure your devices remain secure. This includes:
	+ Keeping the device password-protected
	+ Ensuring the hard drive is encrypted
	+ Locking the device, if left inactive for a period of time
	+ Not sharing the device among family or friends
	+ Installing and updating antivirus and anti-spyware software
	+ Keeping operating systems up to date – always install the latest updates.

**General**

* You must make every effort to comply with copyright and intellectual property rights.