Exeter School

ICT Acceptable Usage Policy

Status:	Approved
Approver:	SLT
Source (author):	GSB
Last review date:	August 2023
SRO:	GSB
Next review date:	August 2024

Exeter School ICT Acceptable Use Policy

Scope

Exeter School provides ICT facilities for pupils and staff for educational and administrative purposes. This policy applies to the use of all ICT equipment (including all school IT equipment and pupil-owned, school-managed iPads), on the school site or used for school-related activities.

Although below sixth form there is no requirement for anyone to bring personal ICT equipment into school, any that is brought in must be used in line with this policy (this includes but is not limited to any personal devices belonging to staff or pupils connected the mobile phone network).

In writing this policy due regard was given to the following publications:

- Keeping children safe in education (2023)
- Meeting digital and technology standards in schools and colleges (updated March 2023)
- Protecting children from radicalisation: the prevent duty (2015)
- UK Safer Internet Centre: Appropriate filtering and monitoring, A Guide for education settings and filtering providers (August 2023)

Staff should ensure they read the full IT policy contained within the Staff Handbook alongside this document.

Objectives

- To promote the safe and responsible use of ICT across all aspects of school life.
- To help ensure that the School's systems and users are protected from any accidental or deliberate misuse of technology.
- To enable Exeter School to comply with its duties in KCSIE and other education-specific guidance.

The School's ICT facilities are primarily intended for educational use and that they can only be used for personal or recreational use if you have permission to do so.

There is no requirement for staff to use their personal devices for school-related activity.

Filtering and monitoring

The School filters internet access on its networks. Filtering prevents users (pupils and staff) from accessing inappropriate content on school systems (including via Wi-Fi). What sites are deemed inappropriate is constantly changing and results from a combination of the Internet Watch Foundation watch list, lists of sites from the home office, the DfE and other sources, and a comprehensive key word list.

Sometimes perfectly appropriate sites are filtered and so are not accessible. The filtering system must not impede learning and teaching. Staff or pupils who require access to any currently blocked site, may request it to be 'unblocked' via the ServiceDesk/deputy head. Sites are evaluated on a case-by-case basis.

The filtering system is regularly tested using the SWGfL filtering testing tool: http://testfiltering.com/

Monitoring allows the school to keep track of any potentially concerning online activity using school systems and take appropriate action where necessary. For example, it can detect when a user in school is using the Wi-Fi to attempt to access an inappropriate site or searching for any potentially concerning or 'risky' terms.

There is automatic reporting of any potentially concerning online activity on school systems. The School may examine these logs, along with stored files, messages and other data stored on the system as part of routine supervision and monitoring, or following any safeguarding concerns, suspected breach of policies or the law.

If you fail to use the ICT facilities in a respectful and appropriate manner, then ICT and internet access may be restricted or suspended. In serious cases, the appropriate authorities may be involved.

Guidance

In an environment of rapidly changing technology, the spirit of this policy is more important than the detail. This policy outlines the way in which we expect you to make use of all digital resources within school.

The primary consideration is that all use of ICT facilities and services must always be respectful and appropriate for a school environment. Respectful towards other members of the school community and towards the systems, and appropriate to staff professional activity or pupils' education.

Key requirements for staff and pupils

You must:

- Only log in using your own username and password.
- Only ever use the facilities for the purpose they were intended (never seeking to make unauthorised changes to systems or software).
- Immediately report any concerns you have regarding online safety (e.g. online bullying, unsuitable and/or illegal material, etc.) to a member of staff.
- Ensure you have your device(s) (see below) with you daily and that they are ready and in a state to support learning (i.e. fully charged):
    - U2: School owned and managed iPads
    - 3F-U5: Pupil owned school managed iPads
    - 6F: Mobile devices compliant with the requirements on screen size, etc
    - 3F-U6: small set of portable headphones
- Observe copyright, and acknowledge the work of others and any sources of information you use in your own work.
- Only print what is required and only when authorised to do so.
- Store/archive work in the designated location (OneDrive, Google Drive or the local network as required).
- Report any technical faults or damaged equipment to a member of staff.
- Lock work stations/log off when unattended.

You must not:

- Share your login details with anyone nor allow them to use your account.
- Attempt to impersonate anyone, or attempt to avoid the School's filtering and monitoring systems.
- Use any equipment, facility or service without the appropriate permission or authorisation from a member of staff.
- Use devices or systems to disrupt or harass others, or in any way which prevents other people from learning or working.
- Share personal information about yourself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc,).
- Take or distribute images of anyone without their permission.
- Connect any device to the network or to another computer unless authorised to do so.
- Attempt to access anything that may be illegal or inappropriate for a school environment.
- Store any copyrighted files or music on the School's systems or subscribe to any online services without appropriate permission.
- Bring in to school, download, or attempt to install any application or programme without permission from a member of staff.
- Publish anything about Exeter School on the internet without the permission of the school.
- If you are in any doubt about anything on policy, you should first seek the advice of members of IT staff.