

-

- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras, still and video
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to the Trust's network and computers.

The Lead IT will monitor the use of all ICT facilities and electronic devices. Members of staff will only use Trust-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school-encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.
- Other general Trust-related work.

Inappropriate use of Trust-owned and personal devices could result in a breach of the Trust's Data Protection Policy.

Inappropriate use of Trust-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the Trust's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the Headteacher and appropriate measures taken.

Trust-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Community Inclusive Trust – **Acceptable Use of the Internet and IT Systems Policy**

Any illegal, inappropriate or harmful activity will be immediately reported to the Headteacher and Lead IT.

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files without permission from the Central ICT Team.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be conducted through authorised school contact channels.
- Take their allocated classroom mobile phone out of the school premises, unless permitted by the Headteacher.

All data will be stored appropriately in accordance with the Trust's Data Protection Policy.

Members of staff will only use Trust-owned electronic devices to take pictures or videos of people who have given their consent.

Staff allocated with a Trust-owned electronic device such as a mobile phone may use it to access personal social media accounts; however, they must adhere to guidance set out within the Trust's Social Media Policy.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the Trust online.
- Avoid disclosing any confidential information or comments regarding the Trust, or any information that may affect its reputability.
- Have the necessary privacy settings applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

Trust-owned devices may be taken home for work purposes where r

Use of a Trust-owned phone for personal use will be permitted for necessary or emergency calls.

Personal use of Trust-owned equipment can be denied by the Headteacher, line manager or Lead IT at any time. This will typically be because of improper use or over-use of Trust facilities for personal reasons.

Where permission has been given to use the Trust equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school/work. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours, provided that disruption to the staff member's work and the work of others is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use and misuse of the facilities as defined in this policy will be reported to the Headteacher, line manager and Lead IT.

Failure to adhere to the rules described in this policy may result in disciplinary action in line with the Disciplinary Policy and procedures.

5. Emails and the

Contracts sent via email or the Internet

During lesson times, unless required for the teaching activity being undertaken, personal devices will be locked away.

In4.96tif/.04 Tf1@ measures.

8. Removable media

Only recommended removable media will be used including, but not limited to, the following:

- USB drives
- DVDs
- CDs

All removable media will be securely stored when not in use.

Personal and confidential information will not be stored on any removable media.

The Central ICT Team will encrypt all removable media with appropriate security measures.

Removable media will be disposed of 13/Lang 24 666.94 Tm0 g0 Gpf2cur

Community Inclusive Trust – **Acceptable Use of the Internet and IT Systems Policy**

- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be changed every 60 days. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
 - Any material that is illegal.
 - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations.
 - Online gambling.
 - Remarks which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false.
 - Any sexually explicit content, or adult or chat-line phone numbers.
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the Central ICT Team, Lead IT, line manager or the Headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the Trust's computers.
- Use or attempt to use the Trust's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the Central ICT Team, line manager or Headteacher. This is in addition to any purchasing arrangements followed according to the Financial Management Policy.
- Use or attempt to use the Trust's phone lines for Internet or email access unless given authorisation by the Headteacher, line manager or Lead IT. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the Internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the Internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher or line manager. This is in addition to any purchasing arrangement followed according to the Financial Management Policy.
- Knowingly distribute or introduce a virus or harmful code onto the Trust's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the Headteacher or line manager. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the Internet or email that may be illegal to do so. This can include computer software, music, text and video clips. If a staff member is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use or attempt to use the communication facilities to call overseas without the authorisation of the Headteacher or line manager.
- Obtain and post on the Internet or send via e.ET62.800000.000008866 0 594.96 8(r)-.04 Tf1 0 f11

Community Inclusive Trust – **Acceptable Use of the Internet and IT Systems Policy**

The Trust's network will be secured using firewalls in line with new DfE guidance, National Cyber

Community Inclusive Trust – **Acceptable Use of the Internet and IT Systems Policy**

The Trust's database systems are computerised. Unless given permission by the Headteacher or line manager, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.