QUEEN'S PARK HIGH SCHOOL

ICT
Policy

Policy Name:	ICT Policy			Review Date: 08/03/2019	Every 3 Years 08/03/2022
Presented to the Resources Committee:	Date: 08/03/2019	Adopted by the Full Governing Body:	Date: 21/03/2019	Chair of Governors Signature:	

Student Information Communication Technology (ICT) Acceptable Use Policy

1. Rationale

Queen’s Park High School is reliant upon computerised information systems to support the day to day running of the school. Computerised systems are used to support teaching and learning across the whole curriculum, manage student and staff information, support business activities and provide information for parents/carers.

ICT offers a powerful learning tool so it is important that staff and students have access to technology to ensure that they benefit from it. Students leaving school require ICT knowledge, skills and awareness to help them be successful in their future careers.

The ICT Policy establishes the expectations and requirements for all users of ICT systems in Queen’s Park High School.

Breaking the school ICT Acceptable Usage Policy may lead to disciplinary procedures being invoked and/or ICT access and facilities being withdrawn.

2. Purposes

The ICT Policy aims to:

- Promote the use and development of ICT.
- Protect the school network and devices from illegal and unauthorised access.
- Protect the school network and devices from viruses and malware.
- Safeguard students and staff from malicious Internet and email usage.
- Safeguard student and staff data stored on the school network.
- Provide a safe ICT environment for teaching and learning.
- To give guidance to staff and students on what is expected with acceptable ICT usage.
- To make clear that students have responsibilities while using ICT. Students and parents/carers must agree to the contract of acceptable ICT behaviour.

3. What is ICT?

The term ICT in this policy document is used to indicate the whole range of technologies involved in information processing and electronic communications and includes the following (this list is not exhaustive).

- Computer hardware devices.
- Internet/Intranet.
- Email.
- Software.
- Projectors.
- Interactive whiteboards.
- Tablet devices.
- Electronic devices such as digital cameras, scanners and printers.
- Telephony.
- Virtual learning environment.
- Website.

The main purposes of ICT at Queen’s Park High School are to:

- Improve and enhance teaching and learning.
- Produce more accessible, high quality teaching materials.
- Assist students in producing work to a good standard.
- Produce high quality documentation across the school and improve administrative practices.
- To give students the opportunity to use different technologies that will be available in the workplace.
- To allow parents and carers to access information easily.
- To allow fast communication and collaboration with others.
- To collect and analyse information.

4. Roles

Role of Staff

The main goal of ICT at Queen’s Park High School is to enhance teaching and learning for all staff and students. Therefore the school will seek to ensure that ICT is used and can be accessed across all curricular areas. It will be an integral part of all faculties and should permeate all areas of the curriculum through the use of computers, Internet, email, software, cameras and so on.

ICT development should therefore be part of all faculties’ schemes of work and staff should highlight activities which involve ICT.

ICT will also be central to the administrative operation of Queen’s Park High School and should be used as a tool to write reports, monitor progress, record marks, keep class lists and record accurate attendance, keep an accurate inventory and any other relevant administrative activities.

It is the responsibility of curriculum leaders to ensure that their faculty has the skills and training required for ICT and how they develop and promote the use of ICT within their teams. Subject leaders should also update schemes of work to ensure that they reflect the use of ICT in their subject area.

Role of Students

At Queen's Park High School our target is to produce students who are confident and effective users of ICT.

To achieve this we will seek to:

- Help students to develop the necessary skills to use ICT.
- Strive to ensure access to ICT for all students across the school.
- Promote interactive methodologies in the use of ICT with students.
- Develop greater independent thinking through the use of ICT.

Students ought to have the opportunity to experience ICT across the full curriculum and staff have a duty to encourage the development of ICT skills in all relevant areas.

The school will support the development of the extra-curricular initiatives which encourage the development of ICT skills. For example, website building, computer clubs, and the Virtual Learning Environment (VLE).

It is the school's policy that students and their parents/carers sign an 'Acceptable Users Policy' document during school enrolment, to use ICT equipment in Queen's Park High School. A copy of this document is at the end of this policy.

This student ICT AUP makes it clear that students have responsibilities when using ICT. If they act in an irresponsible manner they will be held responsible and may have sanctions placed upon them.

Role of Parents/Carers

Parents and carers are integral to the success of ICT at Queen's Park High School and can assist ICT development by:

- Reading carefully and agreeing to the 'Acceptable Users Policy' and returning a signed copy on enrolment.
- Encouraging the development of ICT skills at home where resources are available.
- Checking homework related to development of ICT skills.
- Encouraging their child to discuss the use of ICT at school.
- Where possible, interacting with the Queen's Park High School website and EduLink One and providing feedback on its content and usefulness.
- Supporting the sanctions aspect of the school's policy when their child may have abused the use of ICT in the school.

5. Acceptable Usage Guidelines and Rules

Acceptable Usage Agreement

All staff, students and other users agree to the ICT Acceptable Usage Guidelines. These guidelines must be followed at all times. All computer users have to click ‘OK’ to agree with the AUP before they are allowed to log onto the computer.

Network Monitoring

- All of the systems in Queen’s Park High School are monitored and logged by both automatic systems and through manual checks by the IT Support team. This includes Internet and email checks.

- IT support also use software that monitors computer screens and live activity.

- Emails and Internet logs are monitored for the prevention and detection of unauthorised use. Under normal circumstances, emails will remain private. However, from time to time the IT Support team reserve the right to monitor and open emails and view Internet usage through reporting. This will ensure compliance with the ICT policies and or for the reasons below:

  If Queen’s Park High School suspects and individual:

  - Has been using the email system to send and receive an excessive number of personal communications.
  - Is sending or receiving emails that are detrimental to Queen’s Park High School.
  - Has been spending and excessive amount of time viewing websites that are not work related.
  - Has been accessing inappropriate websites (as broken down in the Internet section below).

- Any computer misuse by staff will be reported to line managers or the Support Operations Manager and Headteacher.

- Please report any security incidents, suspected breaches, unusual computer/network activity or misuse of ICT systems to the Support Operations Manager.

Computer and Network Security

- The school’s network contains information that is personal and sensitive. Access to the information is controlled via user permissions and passwords.

- Never share your passwords with anyone.

- Never log into the network as anyone else.

- Staff and students are only authorised to use those facilities made available to them. No one must attempt to use any facilities, systems or areas of the network that are unauthorised. Such unauthorised access may be treated as gross misconduct.

- Do not allow students to access staff computers. Do not let students use computers that are logged in as members of staff.

- Users must ‘log out’ of systems fully when leaving their devices unattended.

- Never attempt to connect personal equipment to the school network. Only equipment provided by the school is permitted for use on the network.

- Change your password every 30 days to help secure your account and access to personal data.

- Make sure your passwords are strong passwords. They should include upper and lower case characters, numbers and symbols where possible. An example of this format could be jelly22Fi$h.

- Do not save personal staff or student information on laptops, memory sticks or any other device that can be taken off site. All sensitive student and staff information must ONLY be stored on the school network.

- Do not attempt to change system settings or install any software. If you require anything installing or changing please contact the Support Operations Manager.

Internet

- Website access and filtering is controlled via Impero and a Sophos UTM, managed by Queen’s Park High School.

- If you need to access a website which has had the content blocked you must supply IT Support with the details. IT Support will discuss and agree the sites suitability and categorise it for future browsing. The website will be updated on the QPHS whitelists where appropriate.

- Queen’s Park High School does not accept any liability for any loss or damage to any items or monies arising from personal banking or related order issues over the Internet on any computer.

- The use of an Instant Messenger service or chat rooms is not permitted unless strictly work related.

  Inappropriate use of the Internet includes:
  - Any personal use that could cause congestion, delay or disruption of service to any school system or equipment. Examples include data streams such as Internet Radio Streaming and cloud file storage continual uploading/downloading.
  - Using school systems to launch computer based attacks or gain unauthorised access to other systems.
  - Using the school systems for activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, speech, text or images which promote hate or ridicule others on the basis of race, creed, religion, colour, sex, disability, national origin or sexual orientation.
  - The creation, downloading, viewing, storing, copying or transmitting of sexually explicit or sexually orientated materials.

    - The creation, downloading, viewing, storing, copying or transmitting of materials relating to illegal gambling, illegal weapons, terrorist activities and any other illegal activities.
    - Use for commercial purposes or "for profit activities" or other outside employment activity.

Email

- Users should regularly check through their emails to clear down unwanted email as each mailbox is restricted in size.

- All emails that are sent and received are subject to filtering and virus scans both by school systems and Microsoft. All emails are a part of the Office 365 subscription by Microsoft.

- Treat email suspected of being tampered with or from a dubious source with care. Do not open email attachments from unknown sources without checking with IT Support. Don't reply to any dubious emails.

- Please be aware that a disclaimer is automatically added to all outgoing emails stating that emails are sent in confidence and for the addressee only.

  When sending & receiving emails please remember:

    - Email is a very formal means of communication, treat email as though you were engaged in written or verbal communication.
    - Do not make defamatory, racial or sexual remarks about any person or organisation. Emails can be used in evidence in a court of law.
    - Email must not be used to send or receive obscene material.
    - Email is immediate. Please remember this when constructing your emails.
    - Offers and contracts made by email are considered as legally binding.

Social Media

- Social media websites such as Facebook, Twitter, Instagram and Pinterest should not be accessed on the school network other than for work related tasks.

- Social media can be used for marketing the school via it's officially set up accounts.

- Social media can also be used when investigating cyber bullying or other complaints that may arise from parents/carers, students or the community.

Virus and Malware

- Do not use removable media from unknown origins.

- All of the school's computers have AntiVirus installed. This software must be enabled at all times. If an alert via the school's AntiVirus appears on a staff or student computer, a member of IT Support must be notified immediately. A failure to follow these guidelines or deliberate action that causes the school's network to be infected by a virus (regardless of damaged caused) may be treated as gross misconduct.

- AntiVirus signature files are updated daily on workstations and servers.

Backup

- Save all files to the network to make sure that everything is backed up by the schools systems.

- Home areas and shared drives are backed up via several different methods to ensure that data is recoverable. If you need any files restoring please contact a member of IT Support.

Printing

- Please only print when necessary to help save the school money.

- Where printing is essential please print in black and white where possible, as colour costs considerably more.

- Any large print runs or colour printing should be booked in with Reprographics. The Reprographics devices cost less per print and can also process printouts to a higher quality finish. 48 hour notice needs to be given to Reprographics for these requests.

Licenses/Software/Screensavers/Assets

- Do not install unauthorised screen savers to any PC. Screen savers are commonly used for malicious activity and spreading viruses.

- Queen's Park High School will not condone the use of software that does not have a valid license and any employee found to be using, or in possession of unlicensed software will be the subject of disciplinary procedures.

- All computer software acquired by the school must be purchased through the Support Operations Manager.

- No software/drivers can be downloaded by any member of staff/students other than the IT Support team.

- All newly purchased software will be delivered to IT Support so that licenses can be checked and installed on specified workstations by a member of the IT Support team.

- Computer software can only be installed by the IT Support team; under no circumstances can computer software be installed by any other QPHS staff or students. This also includes all laptops and other mobile device owned by Queen's Park High School. This includes any shareware, freeware, public domain software, games, drivers and screen savers and any software received via email.

- Once a computer is deemed ready for disposal all software will be re-used or stored (where the license permits). Hardware will be disposed of in conformance with the WEEE regulations.

- Only IT Support staff are allowed to move/relocate computers so that appropriate software can be added or removed, asset registers updated and any telephony work undertaken.

Mobile Devices and Security of Equipment

- Any laptop or other mobile device issued to a Queen's Park High School member of staff remains the property of Queen's Park High School. The member of staff must sign for receipt of the laptop, adhere to the user policy and return the laptop the IT Support team when requested for health checks.

- Any equipment taken off site is the responsibility of the member of staff that it is issued to. For insurance purposes it is essential that equipment is not left unattended in any vehicle.

- Do not remove QPHS asset stickers from equipment.

- Keep equipment locked up and safe when it is not in use. Do not leave equipment where it can be easily picked up by someone else.

- Missing equipment may have to be reported to the police to obtain a crime number. If any equipment does go missing, please inform the Support Operations Manager immediately.

Compliance with Legislation

All users should be aware of the legislation that Queen's Park High School is required to comply with. Some examples of this legislation are:

- Data Protection Act 1998.
- General Data Protection Regulation 2018.
- Freedom of Information Act 2000.
- Regulations on the Reuse of Public Sector Information 2005.
- Computer Misuse Act 1990.
- Electronic Communications Act 2000.
- Police and Criminal Evidence Act.
- Copyright, Design and Patents Act 1998.
- Protection from Harassment Act 1997.
- Sexual Offences Act 2003.
- Defamation Act 1996.

6. Conclusion

Successful implementation of this policy will ensure that issues relating to ICT are routinely woven into all of Queen's Park High Schools ICT activities, ensuring proper control measures are in place and managed effectively.

7. Message On Staff Computers At Login

QPHS – Staff Computer Acceptable Use Policy

STUDENTS/VISITORS/CONTRACTORS ARE NOT PERMITTED TO USE THIS COMPUTER.

Use of the network - Staff:

1. You must not share your user account details with anyone or log on to a system on behalf of anyone.
2. You must use this computer for work related use. However, limited and reasonable personal use is permitted during non-working hours, i.e. lunch breaks.
3. You must not explore areas of the network where you are not permitted to.
4. Your password should be changed every 30 days, and should be a strong password as described in the ICT Policy.
5. You must not transmit or store any data that infringes copyright laws.
6. Purchasing goods, services or entering into contracts on behalf of QPHS without authority is not permitted.
7. You must not use the QPHS network to trade, or to run a private business.
8. You must not try and gain access to someone else's user account.
9. You must save all files to the Network (Staff Shared & Home areas) to ensure they are backed up.
10. You must not store any student or staff information on a memory stick or portable device. All sensitive data must be stored in the appropriate area on the Network only.
11. You must allow the Anti-Virus scans to complete on devices that you plug into the computer.
12. You must not attempt to connect any personal devices to the QPHS network.
13. You must not attempt to change any computer settings nor bypass any security settings.

Use of the Internet and e-mail:

1. You may use the Internet provided by QPHS for work related research. Personal use is restricted to limited and reasonable use.
2. You must not use the Internet provided by QPHS to access illegal, harmful, derogatory, racist or explicit material.
3. You must not download material that is harmful, illegal, or could bring QPHS into disrepute.
4. File sharing, P2P, and torrent downloads are strictly prohibited.
5. You must not stream music or films from the Internet without prior approval from Network Administrators.
6. You must not use the Internet provided by QPHS to run private businesses.
7. You must observe the rules of e-mail (netiquette).
8. Offensive Language is not permitted and emails containing offensive language will be blocked.
9. You must not send unsolicited, unauthorised e-mails that could invoke QPHS into contract or purchase.
10. You must not use your e-mail account to sign up to websites that deliver SPAM.

INTERNET AND E-MAIL USE IS MONITORED AND LOGGED BY SECURITY SYSTEMS CONSTANTLY. LOGS ARE ALSO LOOKED AT MANUALLY BY NETWORK ADMINISTRATORS AND ANY MISUSE WILL BE REPORTED,

Software:

1. You are not permitted to install any software on any QPHS device.
2. All software installation requests must be made to the Network Manager.
3. All software must be correctly licenced. Proof of licence will be required.

Home Use:

1. Where a device is portable (e.g., laptop) and is booked out to you, you may use this device at home for work related use only.

For a detailed explanation of the QPHS ICT Acceptable Use Policy please refer to the Policies on the staff network shares.

8. Message On Student Computers At Login

QPHS – Student Computer Acceptable Use Policy

Use of the network – Students:

1. I will use computers only for school work.
2. I will not enter any computer room unsupervised.
3. I will not turn computers on or off without permission.
4. I will only use approved network software.
5. I understand that all activity on the network is recorded and that the administrators have the right to view my files and may disable my account.
6. I will not attempt to change any computer settings nor bypass any security settings.
7. I will not remove any cabling or connections from any equipment.
8. I will not disclose my password to other students.
9. I will not interfere with other users work or accounts in any way.
10. I will not store any copyrighted material on the school network and will adhere to copyright laws when using school computers.
11. I understand that any copyrighted or inappropriate materials found will be deleted by the administrators without warning. Constant abuse of copyright and inappropriate materials will result in a network ban.
12. I will only access school work from memory sticks. Any other files will not be accessed while in school.

Use of the Internet and e-mail:

1. I understand that access is a privilege and requires responsible behaviour.
2. I understand that use of the Internet must be directly related to my school work.
3. You must not use the Internet provided by QPHS to access illegal, harmful, derogatory, racist or explicit material.
4. I will not attempt to shop online nor try to download files that are unsuitable for school use as determined by a teacher or administrator.
5. While using the Internet I will not disclose any personal details without direct permission from a teacher.
6. I will not send any offensive messages or pictures.
7. I will not use any Internet sites that bypass any network security settings.

- I understand that all teachers and support staff will monitor and enforce this policy.
- I understand that evidence of serious inappropriate computer use resulting in a ban or reduced access will be sent to my parents/carer and recorded on my behaviour record.
- I understand that violations of the above will result in reduced access, a ban from the Internet or school network and where appropriate police or local authorities may be involved.
- I understand that I am liable for any wilful damage to equipment and parents/carers will be sent the bill for the cost of any repairs.

Use of the network – Staff:

The school staff handbook has detailed guidance about, the School's Acceptable Use Policy. The policy is designed to help employees and other users (e.g. visitors, contractors) understand the ways in which they are and are not allowed to use the QPHS IT and communications systems.

9. ICT Acceptable Use Policy (Student/Parent/Carer Signed Document)

Student ICT Acceptable Use Policy - *Please read carefully and sign below.*

Students will not be able to use the computer network or Internet in school until they hand this signed contract to their Group Tutor or Student Services, who will return it to IT Support.

Use of the network:

1. I will use computers only for school work.
2. I will not enter any computer room unsupervised.
3. I will not turn computers on or off without permission.
4. I will only use approved network software.
5. I understand that all activity on the network is recorded and that the administrators have the right to view my files and may disable my account.
6. I will not attempt to change any computer settings nor bypass any security settings.
7. I will not remove any cabling or connections from any equipment.
8. I will not disclose my password to other students.
9. I will not interfere with other users work or accounts in any way.
10. I will not store any copyrighted material on the school network and will adhere to copyright laws when using school computers.
11. I understand that any copyrighted or inappropriate materials found will be deleted by the administrators without warning. Constant abuse of copyright and inappropriate materials will result in a network ban.
12. I will only access school work from memory sticks. Any other files will not be accessed while in school.

Use of the Internet and e-mail:

1. I understand that access is a privilege and requires responsible behaviour.
2. I understand that use of the Internet must be directly related to my school work.
3. You must not use the Internet provided by QPHS to access illegal, harmful, derogatory, racist or explicit material.
4. I will not attempt to shop online nor try to download files that are unsuitable for school use as determined by a teacher or administrator.
5. While using the Internet I will not disclose any personal details without direct permission from a teacher.
6. I will not send any offensive messages or pictures.
7. I will not use any Internet sites that bypass any network security settings.

Student ICT Acceptable Use Policy – Contract.

I understand that all teachers and support staff will monitor and enforce this policy.

I understand that evidence of serious inappropriate computer use resulting in a ban or reduced access will be sent to my parents/carer and recorded on my behaviour record.

I understand that violations of the above will result in reduced access or a ban from Internet access or school network use. Where appropriate police or local authorities may be involved.

I understand that I am liable for any wilful damage to equipment and parents will be sent a bill for the cost of any repairs.

Student signature: ……………………………Tutor Group:…………… Date: …………………..…

Print Name: ………………………………………………..…..

Parent or Carer signature: ………………………………… Date: …………………………

Print Name: ……………………………………………………..

ICT – Student Computer/Network Misuse Procedure

Misuse of ICT is either found by IT Support monitoring or after being reported in by a member of staff.

The severity of misuse is assessed by IT Support.

Low Impact Misuse
The teacher/tutor of the lesson (tutor if in own time) is informed about ICT misuse so that they can warn the student about future conduct.

Severe Misuse
The student account will be immediately banned and the student reported to Key Stage Manager and/or the Headteacher. Misuse is also reported to Parent/Carer.

The student is monitored for misuse for the rest of the academic year. If another incident of misuse occurs in the academic year:

The severity of misuse is assessed by IT Support.

Low Impact Misuse
The student is reported to their Key Stage Manager. The student will need to re-sign the Student ICT AUP contract in the IT Support Office.

The Key Stage Manager may decide to ban the student from the network/Internet for a week period.

Severe Misuse
The student account will be immediately banned and the student reported to Key Stage Manager and/or the Headteacher. Misuse is also reported to Parent/Carer.

The student is monitored for misuse for the rest of the academic year. If another incident of misuse occurs in the academic year:

The severity of misuse is assessed by IT Support.

Low Impact Misuse
The student is reported to their Key Stage Manager and SLT. The student will be banned from the network/Internet for the remainder of the half term/full term.

Parents/Carers will be informed of the action taken and repeated misuse of ICT in school.

Severe Misuse
The student account will be immediately banned and the student reported to the Key Stage Manager and/or the Headteacher. Misuse is also reported to Parent/Carer.

The student is monitored for misuse for the rest of the academic year. If another incident of misuse occurs in the academic year:

The severity of misuse is assessed by IT Support.

Low Impact Misuse
The student is reported to their Key Stage Manager and SLT. The student will be banned from the network/Internet for the remainder of the academic year.

Parents/Carers will be informed of the action taken and repeated misuse of ICT in school.

Severe Misuse
The student account will be immediately banned and the student reported to the Key Stage Manager and/or the Headteacher. Misuse is also reported to Parent/Carer.

Severe Misuse

In all cases of severe ICT misuse a network/Internet ban will be issued. Severe misuse can result in the permanent ban of ICT equipment in school.
Severe misuse of ICT can also result in student exclusions.
In severe misuse incidents, where appropriate, police or local authorities may be involved.

Academic Year End

IT Support will meet with Key Stage Manager to discuss what is going to happen with students that were permanently banned from the network/Internet for the remaining academic year. Parents/Carers may be asked to come in and discuss plans for ICT access going into a new academic year.

Examples of Low Impact ICT Misuse

The list below gives some examples of low impact ICT misuse (this list is not exhaustive):

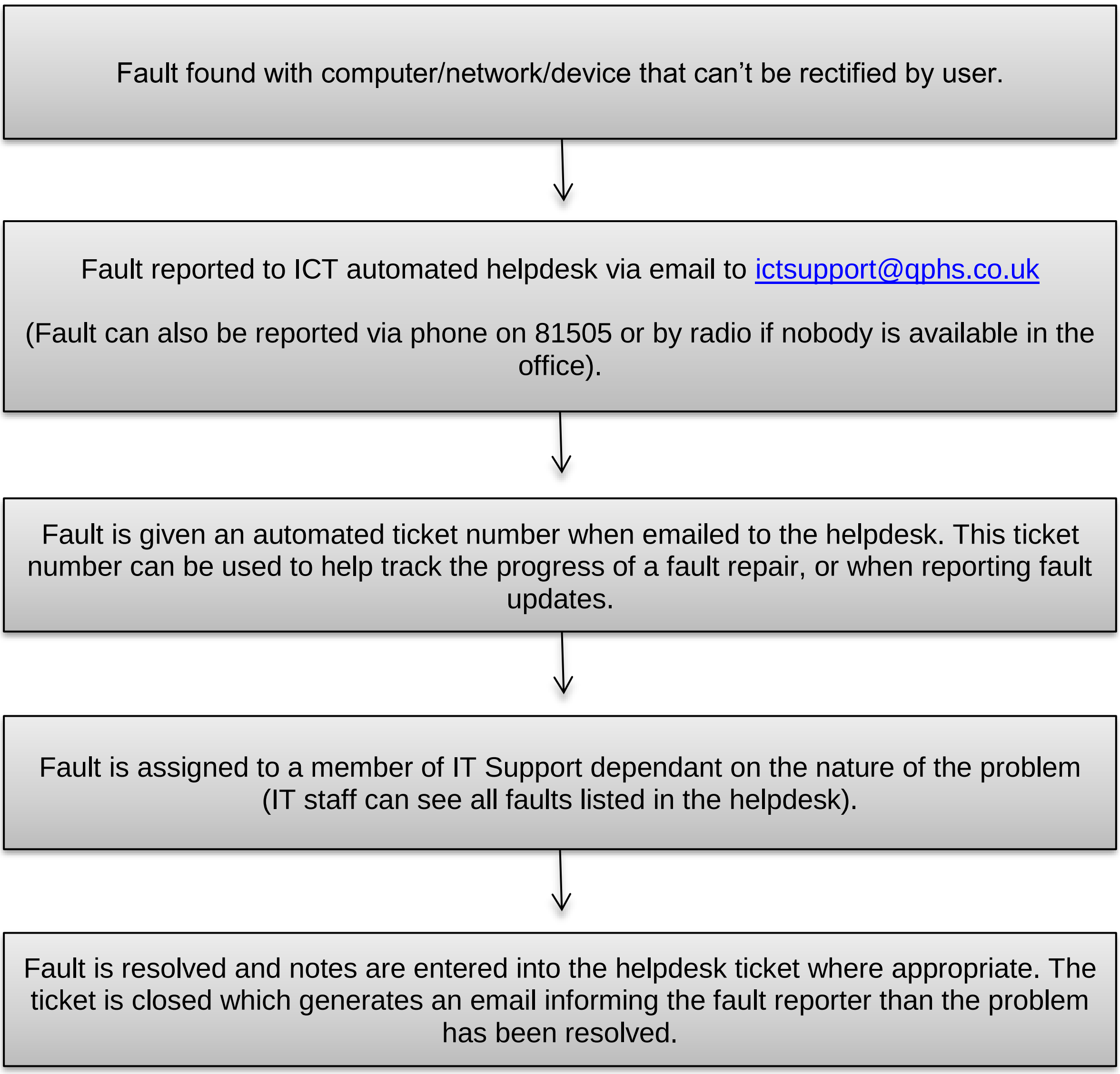
- Playing games on the Internet.
- None school work related browsing of the Internet.
- Removing cables, keyboards and mice from computers.
- Logging in as somebody else/renaming peoples saved files.
- Email misuse.
- Wasting print credits.

Examples of Severe ICT Misuse

The list below gives some examples of severe ICT misuse (this list is not exhaustive):

- Bypassing network security by using Proxies.
- Accessing sexually explicit content.
- Deliberate damage to the ICT equipment in school.
- Trying to bypass security policies to allow ‘administrative’ access to the computer or network.

ICT – Fault Logging Procedure



Fault found with computer/network/device that can't be rectified by user.

Fault reported to ICT automated helpdesk via email to ictsupport@qphs.co.uk

(Fault can also be reported via phone on 81505 or by radio if nobody is available in the office).

Fault is given an automated ticket number when emailed to the helpdesk. This ticket number can be used to help track the progress of a fault repair, or when reporting fault updates.

Fault is assigned to a member of IT Support dependant on the nature of the problem (IT staff can see all faults listed in the helpdesk).

Fault is resolved and notes are entered into the helpdesk ticket where appropriate. The ticket is closed which generates an email informing the fault reporter than the problem has been resolved.