Queen Anne High School
Information and Communications Technology (ICT) Policy Draft

Information and Communications Technology (ICT) is an essential resource to support learning as well as playing an important role in the lives of young people. Schools need to use these technologies to prepare young people with the skills to access life-long learning and employment, and to ensure young people are confident in the safe use of technology.

ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within society. The internet technologies young people are using both inside and outside the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and web functionality

Whilst exciting and beneficial both in and out of the school, much ICT (particularly web-based resources) is not constantly policed. All users need to be aware of the risks associated with the use of these internet technologies.

At Queen Anne High School, we understand the responsibility to educate young people on e-Safety issues: teaching appropriate behaviours and critical thinking skills to enable them to remain safe and legal when using the internet, and related technologies in and beyond the context of the classroom.

OUR AIMS

- To provide simple, clear guidelines for using the school network, e-mail and internet services
- To protect young people from harmful sites, people and influences while using the internet or e-mail
- To provide young people with a framework for using programs and equipment appropriately
- To provide guidelines for educational internet use

- To provide guidance on the use of personal ICT equipment
- The internet is constantly evolving and we must remain alert to developments in internet usage, and their impact on internet safety

HOW GOOD IS OUR SCHOOL? (4th edition) – DEFINITIONS:

Digital learning is learning which is supported and enhanced by a range of digital technology and approaches. It can focus on one or more particular technologies. It may focus on classroom use or anywhere-anytime access. It may include features and approaches that are used to develop independent learners.

Digital literacy encompasses the capabilities required for living, learning and working in a digital society. It includes the skills, knowledge, capabilities and attributes around the use of digital technology which enable individuals to develop to their full potential in relation to learning, life and work. It encompasses the skills to use technology to engage in learning through managing information, communicating and collaborating, problem-solving and being creative, and the appropriate and responsible use of technology.

Digital technology is the term used to describe those digital applications, services and resources which are used to find, analyse, create, communicate, and use information in a digital context.

Digital teaching means educators providing and supporting enhanced learning opportunities through use of digital technologies

GLOW

The implementation of 'Glow' (the Scottish Schools Education Platform) provides young people and teachers with a safe and secure online education community, allowing for networking and learning. Glow accounts for pupils, staff and parents have been provided. This education platform is a core element of the Curriculum for Excellence. It allows for easy access to high quality teaching resources with material built specifically for the Scottish curriculum as well as offering access to personalised learning opportunities for our teachers and pupils. Access via Glow is constantly monitored and any breach of the terms and conditions will result in being blocked from this valuable resource.

BRING YOUR OWN DEVICE (BYOD)

In Queen Anne High School, we recognise that the way in which we access information has changed in recent years. Access and use of mobile technology has increased. Resources including: laptops, tablets and mobile devices can provide young people and their teachers with valuable opportunities to access the internet, manage their work, and enhance learning.

Within this context young people and staff will be allowed to connect to the Fife Council Wi-Fi using their own personal devices to access the internet for educational use. Young people and staff will be expected to use devices in accordance with this ICT Policy, and must agree to be bound by the rules and requirements set out below.

OVERVIEW

Pupil Agreement – Pupils must agree to the contents of the school's ICT Policy by agreeing to the conditions of the acceptance form before they are permitted to use their own device. The school will operate an "opt out" approach, whereby the school will assume acceptance of the ICT Policy unless the pupil specifically – and clearly, in writing – opts out. The Policy is available for parents to view on the school website.

Lost, stolen or damaged – Pupils who bring their own devices into school do so entirely at their own risk, just like any other personal item. Queen Anne High School will not accept any responsibility for devices that are misplaced, lost, stolen or damaged. Many devices have a 'Location Finder' app and it is recommended that this feature is enabled to aid tracking where ever possible. It is also recommended that such devices are fully insured to cover loss and damage outside of the home.

Security and Care – Pupils are responsible for the proper care and use of their own device and are responsible for the adequate security and safety of their own device whilst in school, keeping it with them at all times when required or securing properly in their own locker (if appropriate). Pupils should not share or lend their device to other pupils. We recommend a sturdy case for any devices brought in to school

Educational use – Devices will only be used for educational purposes to support learning during the timetabled school day. It will be at the teacher's discretion as to when these devices may be used by a pupil within school. Pupils will respect a teacher's decision and turn off their device when requested to do so. For safety and equity reasons, school staff will strongly advise young people to use Fife Council Wi-Fi, rather than the young person's own data, when accessing the internet in class.

Audio, Photographs and Video – Pupils will not use their device to record audio or take photographs or video of other pupils or members of staff without their permission. Pupils will not send or upload such media without permission.

Internet Usage Policy – school staff will advise young people to use their devices to access the internet **only** through the Fife Council network. Pupils will adhere to the school's ICT Policy whilst in the school. In addition, pupils will not access any inappropriate material that may or may not already be downloaded onto their device.

Pupils breaching the ICT Policy – If a pupil breaches the ICT Policy or if a member of staff feels that they are likely to have breached this policy then the pupil's device will be confiscated and held at Reception. The pupil's parent or carer may be contacted to come into school to collect the device. Subsequent breaches of this policy by the same pupil may result in that pupil no longer being permitted to bring in their own device.

THE POLICY:

1 About this Policy

1.1 In Queen Anne High School we recognise that many pupils have personal mobile devices (such as tablets, smartphones and handheld computers) which could be used for learning purposes. Using such devices could have significant potential benefits for both pupils and teachers, including increased learning flexibility in permitting such use. It is noted however, that the use of personal mobile devices for learning by pupils gives rise to

increased risk in terms of the security of school IT resources and communications systems, and the protection of confidential information.

1.2 This Policy covers all staff and pupils in Queen Anne High School which is based on the Fife Council ICT Policy

1.3 Pupils may use a personal mobile device for learning purposes, if they accept the declaration at the end of this policy and adhere to its terms via the "opt out" approach.

2 Personnel responsible for this Policy

2.1 Before finalising this policy we engaged with a sample group of staff, pupils and the Parent Council. Our Better Relationships, Better Learning, Better Behaviour Guidelines and our Anti-Bullying Guidelines underpin our approach to this.

3 Scope and purpose of the Policy

3.1 This Policy applies to pupils who use a personal mobile device including any accompanying software or hardware (referred to as a device in this Policy) for learning purposes. It applies to use of the device both during and outside school hours whilst on the school site.

3.2 This Policy applies to all devices used to access the council network which may include (but are not limited to) smartphones, tablets, and laptop or notebook computers.

3.3 The purpose of this Policy is to protect the Fife Council network while enabling you to access the network using a device. This Policy sets out the circumstances in which Fife Council may monitor your use of the network, access your device and retrieve, remove or destroy data on it and the action which will be taken in respect of breaches of this Policy.

3.4 Breach of this Policy may lead to the school revoking your access to school systems, whether through a device or otherwise or whatever is deemed necessary as per the school's Policy.

3.5 Some devices may not have the capability to connect to the Fife Council network. There is no obligation for Fife Council or Queen Anne High School to modify its systems or otherwise assist pupils in connecting to the network.

4 Connecting devices

4.1 Connectivity of all devices is overseen by the Fife Council Business Technology Solutions (BTS) but managed by each individual school.

4.2 Fife Council reserves the right to refuse or remove permission for your device to connect with the network. BTS will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, the school, our pupils, our staff, our systems, or sensitive school data at risk or that may otherwise breach this Policy.

4.3 Young people will be advised by their teachers to use Fife Council Wi-Fi when using their own device – or a school device – as part of a school lesson

4.4 Devices will log in by authenticating to Fife Council's network via school wireless access points. For Queen Anne High School, this will be using an individual's Fife Council login usernames and passwords via Active Directory.

5 Monitoring

5.1 Once authenticated to the network all devices will be subject to normal Education Web Filtering and the monitoring that goes with it.

5.2 The school reserves the right to monitor and act upon any content found on a device which is deemed in breach of this Policy. This may include reviewing or erasing content in order to prevent further misuse or to ensure compliance with Policy.

5.3 By accepting this Policy, pupils agree to such monitoring. Pupils who do not accept this Policy must actively "opt out".

6 Security and Care

6.1 Pupils and staff choosing to bring in their own device do so at their own risk. Queen Anne High School cannot take responsibility for any theft, loss or damage to these devices.

6.2 Owners would be advised to secure appropriate insurance on any device they choose to bring into school.

6.3 Pupils and staff must not use electrical points to re-charge their personal ICT equipment. This is in contravention of the Electrical Regulations that govern this school and Fife Council.

7 Technical Support

7.1 The School's Technician Service will not provide any technical support for BYOD devices. Whilst the School's Technician Service will provide support for the wireless provision within the school, this does not extend to support for individual devices connectivity, not owned by the school.

WEB SAFETY

Many people enjoy accessing the Internet, but it is worth remembering to keep safe while in cyberspace. You might think you know a great deal already about the internet, but it is worth bearing a few things in mind:

- Many of us enjoy access to the web via a computer at home, school or even via our mobile phone. It is important to think about what kind of information you give out
- Never give out any personal information such as your home address, phone number or school to anyone you talk to online, even if you are offered free gifts, samples or information
- If you have your own website or pages on a social networking site such as Facebook, remember that these are public sites and anyone can see them
- Always think carefully about what you put on your site especially photos. Instead of putting up a picture of yourself you could draw an image or upload an abstract design to protect your identity
- Remember that people who contact you may not be who they say they are. Anyone can say that they share your interests and are the same age, but not everyone is as they seem
- Never arrange a face to face meeting on your own with anyone you have met on the Internet. If they want to meet with you, tell your parents/carers
- Do not respond to threatening or obscene messages. No matter how irritating or rude they are – tell your parents/carers, block the individual and report them to the site administrator
- Be careful if you receive an email message from someone you do not know. It may contain a virus which could damage your device

ZIP IT, BLOCK IT, FLAG IT

- **Zip it**: Keep your personal stuff private and think about what you do or say online
- **Block it**: Block people who send nasty messages and do not open unknown links and attachments
- **Flag it**: Flag up with someone (parent/carer) you trust if anything upsets you or anyone asks to meet you in person

INTERNET AND PLAGIARISM

Plagiarism means copying or using other people's work and then trying to pass it off as your own:

- Any materials sourced from the Internet must be clearly identified as such, i.e. you must acknowledge/reference your sources of information. Ask your teacher if you require advice on this matter.
- Be aware that copying others' work and submitting it as your own is cheating and is a serious breach of school expectations.
- The Scottish Qualification Authority treats plagiarism very seriously. If plagiarism is identified by the S.Q.A. one of the following penalties will be applied:
    - Cancellation of all your subject entries for that year
    - Cancellation of the entry of the subject/level concerned
    - The piece of work will be awarded zero marks
    - A warning will be issued

QUEEN ANNE HIGH SCHOOL
PUPIL ICT AGREEMENT

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies (e.g. smartphones, tablets, and laptop or notebook computers), etc. for educational purposes to support learning during the timetabled day
- Ringers/notifications will be switched to silent whilst in school and I will not respond to, or initiate, any message or call whilst I am in class
- I will respect a teacher's decision and turn off my personal mobile device when requested to do so
- I agree to use Fife Council Wi-Fi when using my own device – or a school device – as part of a school lesson, as strongly advised to do so by my teacher
- I will not download or install software on school technologies
- I will not access materials which will put a strain on the network and limit internet access for other users
- I will only log on to the school network (whether wired or Wi-Fi) with my own user name and password
- I will be responsible for any use of my 3G/4G network/use of my personal data allowance. I understand that the school cannot be responsible for monitoring my use of my mobile data, nor am I responsible for any costs/penalties for excess use incurred
- I will not reveal my password to anyone
- I will only use my school email address
- I will not give out any personal information such as name, phone number or address.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use
- I will not deliberately browse, download/upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network without prior permission
- I will ensure that my online activity, both in school and outside school, will not cause the school, staff, pupils or others distress or bring them into disrepute
- I will always respect the privacy and ownership of others' work on-line
- I will not attempt to bypass the Council's internet filtering system
- I will not charge my device in school. I will ensure my device is sufficiently charged before coming to school
- I will not use my device to play music when travelling to and from classes and understand this may only be used in class with the express permission of the class teacher
- My mobile phone should not be used or seen between classes
- I understand that all my use of the internet, email and other related technologies can be monitored and logged and can be made available

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted. Sanctions may include temporary removal of my personal device and/or the blocking of internet, email, network access for a time period depending on the severity of the offence
- I understand that subsequent breaches of this policy may result in me no longer being permitted to bring in my own device
- I understand that this agreement applies to use of mobile devices both during and outside school hours whilst on the school site
- I understand that Queen Anne High School takes no responsibility for any misplaced, lost, stolen or damaged personal mobile devices brought on to the school site
- I understand that it is my responsibility to ensure that insurance on any mobile device brought into school has been considered
- I understand that members of staff have the right to remove my personal mobile device if there is reason to believe I may be in violation of the school ICT policy
- I understand that some devices may not have the capability to connect to the Fife Council network and there is no obligation for Fife Council or Queen Anne High School to modify its systems or otherwise assist pupils in connecting to the network

……

Pupil Declaration

I have read and agree to follow the School's ICT Policy to support the safe and responsible use of ICT at Queen Anne High School.

I understand that this is an "opt out" Policy, whereby if I object to, or do not wish to be bound by its terms and conditions, I must inform the school immediately to opt out of the Policy. You must inform your Guidance PT in writing.

Please read this ICT policy very carefully. Any misuse of the Policy will result in sanctions being imposed depending on the severity of the breach:

- Permanent or temporary withdrawal of access to the school's computer facilities
- Parent or carer contacted
- Restrictions on your use of school ICT equipment

For website as foreword to ICT policy and inclusion in the E-Bulletin:

Dear Parent/Carer

ICT including the internet, learning platforms, email and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and follow the terms of the agreement. Please note that this is an “opt-out” Policy, whereby if your or your child objects to, or do not wish to be bound by its terms and conditions, you must inform the school immediately in order to opt out of the Policy. Any concerns or requests for further explanation can be discussed with Guidance or a member of the Senior Leadership Team (SLT).

STAFF ICT ACCEPTABLE USE AGREEMENT / CODE OF CONDUCT

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in this school. This Policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to adhere to this policy at all times. Any concerns or clarification should be discussed with your link DHT.

- I will only use the school's email / internet / intranet / learning platform and any related technologies for professional purposes
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number and personal email address to pupils
- I will only use the approved, secure email system for school business
- I will ensure that personal data is kept secure and is used appropriately
- I will not install any hardware or software without permission from the Senior Technician
- I will ensure that personal data (such as data held on MIS/Guidance) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or a Depute. Personal or sensitive data taken off site must be by encrypted USB device
- I will not browse, download, upload or distribute material that could be considered offensive, illegal or discriminatory
- Images of pupils and/or staff will only be taken, stored or used for professional purposes in line with school policy and with written consent of the parent/carer, or staff member. Images will not be distributed out with the school network without the permission of the parent/carer, staff member or Headteacher
- I understand that all my use of the internet/intranet, email etc. can be monitored, logged and made available on request
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's ICT Policy and help pupils to be safe and responsible in their use of ICT and related technologies
- I agree to follow this code of conduct and to support the safe use of ICT throughout this school
- I will be mindful that the downloading or streaming of videos, radio or music through the school's network affects the bandwidth available to other users and must only be carried out if required for educational purposes

Bring Your Own Device (BYOD) /Anytime, Anywhere Learning (AAL) FAQs

Question 1

"I understand that all my use of the internet, email and other related technologies can be monitored and logged and can be made available".

What does it mean by 'other related technologies'? With regards to email, is that Fife Council email or is it your own person emails (Hotmail, iCloud, Gmail, etc.). Who are the logs being made available to, what security are Fife Council putting in place to prevent data breaches, can staff members view their own logs and if there are data breaches, what/will Fife Council admit liability to loss of personal data which could affect future or prior earnings? (E.g. Bank details)

Response

Fife Council will be able to see what sites are logged into by each user and what downloads / software etc. the internet is used to access. Any personal details being used whilst using any app or piece of software are not monitored. All of this access will be controlled through internet filtering and security in exactly the same way that it is from every other school owned device.

Question 2

How will we ensure equity for pupils without their own devices and avoid any stigma of borrowing a school device?

Response

The school is undertaking an ongoing programme, to ensure that all Curriculum Areas have enough devices for this reason and are available for use by pupils in each department. We are also prioritising PEF funds in 2020-21 for this purpose.

Question 3

How will we manage the impact of mobile devices needing charged during the school day if pupils are using a lot during a day?

Response

The policy allows charging of BYOD devices via PCs but not electrical sockets, and devices must not be left unattended.

Question 4

How will we monitor and manage the impact on the network of all these extra devices and the potential use for non-educational purposes e.g. streaming of music during breaks/lunchtimes?

Response

The 4-6 week pilot in August and September 2020 with reduced pupil capacity will be used to allow us to assess the impact of how AAL will affect network usage in the school. We/Fife Council will be monitoring network traffic to determine what sites are being used, when peak times are etc. There will also be a level of responsibility on the school to be clear that staff and pupils should be using the network for professional and curricular needs and not for personal access. Any issues and any noticeable slowing down of the network should be reported to Technicians who will liaise with Fife Council IT to investigate and seek a resolution.

Question 5

How can staff monitor appropriate usage? For all that the pupils will be asked to sign an agreement, what about the pupils that already 'bend the rules' on having their phones out in class, and what happens when they take a video if there is a confrontation in class between a pupil and a member of staff - this could lead to some awkward situations with parents/carers, and put that staff member in a very difficult position.

Response

Normal classroom management procedures apply.

Question 6
The ICT Policy states that teachers can remove the device if the pupil is misusing it. That is already quite a challenge with some pupils when there's no current Policy in place and may prove even more challenging when they think they are allowed devices in class.

Response
Normal classroom management procedures apply.

Question 7
What if parents don't want their children to use their devices in class?

Response
It should not be regarded as compulsory to bring a device. Devices have been purchased and are available for use in each department for lessons requiring use of devices, should a pupil not have brought their own.

Question 8
Will devices be loaned out for pupils to take home?

Response
No

Question 9
Is there a minimum/certain spec for devices to be able to connect to the network?

Response
Devices only need to have the ability to connect to Wi-fi. Spec will only be an issue if the school decides that specific cloud-based software is to be used for educational needs.

Question 10
Can we insist that certain anti-virus software is on devices that will be connected to the network? How could this be policed?

Response
It is unlikely we can insist on this nor do we really need it. Any personal devices that are being used will not be able to access any mapped drives or internal storage but will only have a direct line out to the internet so we manage the risk to an extent. Sophos web filtering will manage traffic to and from the internet. There can be no file sharing between devices through the Wi-fi as devices will not be able to see each other. Essentially we can recommend anti-virus, but that is about it.

Question 11
Could we be compromising software licensing agreements if we have pupils using their own devices to access systems via the network?

Response
It will depend on the software that classes intend to use and the licences we have in place. If in doubt regarding a particular piece of software, please seek advice from the Technicians.

Question 12

Are we able to stop “bandwidth hogging activities” such as file sharing and large file downloads?

Response
Activities such as these will be monitored and highlighted to us by IT. The monitoring software can identify whether this is specific to a few individuals or to a more widespread group. We may find that some devices will need to download updates to be able to run certain bits of software if required. Pupils may also be likely to pull files from GLOW but this is no different to doing it on a school device.

Question 13
Will we be able to increase our bandwidth if implementation of the BYOD affects web access?

Response
There is a WAN replacement project ongoing just now which has taken into account moves towards BYOD. IT are continuing to explore these options going forward.

Question 14
Will step-by-step guidelines be provided for connecting own devices to the internet through the school network together with common issues/troubleshooting FAQs?

Response
Yes, although it will quite simply be a landing page from which users will authenticate. IT will work with the school to iron out any FAQs which should arise from the pilot.

Question 15
Can we define “offline” times when access to the school network via personal devices is not allowed e.g. pupils streaming music at break times?

Response
This can be done but it is hoped that the pilot will identify whether this is a genuine problem or not. Pupils are not able to access music streaming services under their access rights. All access and filters will remain the same for pupil’s accessing the school Wi-Fi as they are presently when logged in to the network on any school devices.

Question 16
Is there CPD available for teachers on embedding technology into the curriculum and making best use of mobile devices?

Response
The Education and Children’s Services ICT Skills team regularly run Office365/SharePoint/GLOW courses on the CLMS/CPD system. We also have about 30%-40% of staff trained as Microsoft ambassadors. There are regular webinars on the use of Teams, One Note jotters and a wide range of digital pedagogy. Please contact Sarah Clark, Gareth Surgey and/or Nicola Copland for further details.

Question 17
How many mobile devices can our Wi-Fi network support at once?

Response
We are limited by the amount of devices accessing each Wi-fi point. At present we advise no more than 20 devices per Wireless Access Point. However, the Pilot will reveal what our capacity is and how sustainable particular points are. We are increasing the number of WiFi hubs throughout the building.

Appendix 1:

QAHS REMOTE LEARNING SUPPORT GUIDELINES

The following guidelines have been developed by the Digital Working Group to help support and protect staff as we all increase usage of remote learning.

As we develop Remote Learning as a school, there are several online options including: setting work or providing access to online resources through Teams, video tutorials for learners to work through at their own pace and live lessons via video conferencing. Teacher and learner skills in the use of digital tools and access to devices/wifi will influence the way work is set.

There are two main ways in which work can be planned for learners: **Synchronous and Asynchronous.**

- **Synchronous distance learning** occurs when the teacher and learners interact in different places but at the same time (usually via video conferencing). Learners are generally required to log on to their computer during a set time
- **Asynchronous distance learning** occurs when the teacher and learners interact in different places and at different times. Teachers and learners complete their work whenever it is suitable for them. Instruction can be given in a variety of ways.

Asynchronous learning may be easier in the current context especially if learners are sharing devices with siblings/parents and have limited access online. Setting work for the week with a variety of tasks will also help learners plan for all their subjects and share what they have completed later in the week by uploading files or photos of their written work for feedback.

Communicating with learners
Interactive digital communication with learners should only be via Glow. Safeguarding is essential and this platform is nationally managed with safeguarding is at it's core. Email via glow email addresses enables direct 1-1 contact with a learner and Teams provides a great platform to communicate with a class (direct 1-1 chat feature is not enabled in Teams without the rest of the class seeing the communication).

Twitter can be used to direct learners and parents to learning materials on Glow. It is recommended that this is done via a department or faculty Twitter account which has more than one member of staff accessing. Please reach out to the Digital Working Group should you need help with this.

Teachers should not be using their personal social media accounts for contact with pupils.

Online Lessons for learners
This can be done using Teams meetings. These can be live lessons, or pre-recorded (using PowerPoint recorder to add audio to your slides, again, reach out to the Digital Working Group for help with this). Many learners are likely to have shared access to digital devices so pre-recording lessons will help ensure the lesson is accessible to many more learners. Not all may have access to a digital device when a live lesson is scheduled. Glow has turned off the option to have a live lesson recorded for your safety. Learners may however screen record from their phone so be please be aware of this. There is no expectation that teachers will host live lessons for learners, but if you choose to teach a live lesson there is

support within the QAHS Staff Team on setting a 'meeting' and hosting via Teams. Some key things to remember are:

- Learner cameras are turned off by Glow for safeguarding (you may also wish to turn your camera off so learners can hear, but cannot see you)
- Within Teams there is an option to blur your background, or change it, so that learners cannot see your home environment, or anyone who may enter the room
- Remove family photos from your room, if not using blur background.
- It may be useful to have another member of staff in the live lesson to monitor the chat, or provide technical support during the lesson if needed.

Teachers should only use video conferencing via Glow. Other tools such as Zoom, WhatsApp and Skype do not have the safeguarding and encryption required to keep learners and staff safe.

Parent/Carer Emails
Emails via Glow should only be from learners. Please encourage parents to contact their child's Guidance PT as the main point of contact. The GPT will then share with relevant staff.

CPD
There is a wealth of Digital CPD resources outlined in the QAHS Staff Team (cpd channel) to help and support staff to develop their skills and support during this time of Remote Learning.

Key support guidance for reference:

GTCS:
http://www.gtcs.org.uk/web/FILES/teacher-regulation/professional-guidance-ecomms-social-media.pdf

Education Scotland:
https://education.gov.scot/education-scotland/news-and-events/education-scotland-update-regarding-covid-19/

EIS:
https://www.eis.org.uk/Coronavirus/WFHGuidelinesIMT
https://www.eis.org.uk/Health-And-Safety/COVID19

SSTA:
https://ssta.org.uk/wp-content/uploads/2020/03/Member-Bulletin-Working-from-Home.pdf
https://ssta.org.uk/social-distancing-further-information-advice/