Remote working

Guidance for specialist colleges

Introduction

This document has been prepared by Jisc subject specialist **Rohan Slaughter** to assist specialist college leaders with IT and technology related decision making that is important to initiate or maintain remote working and general business continuity at this challenging time. Rohan is a former specialist college assistant principal and used to lead the Technology team at Beaumont College. This document has been produced quickly, it is not aiming to be complete, and it will be iterated. If your college is a Jisc member organisation we can provide advice and guidance via your **Jisc account manager**. Note that if we have a recent Jisc infrastructure review in hand for your College this will improve the quality and the speed of any response we can make.

This information is being put out quickly, rather than taking additional time to polish and check it. We felt it would be useful to be 95% correct now, rather than 100% correct at some future point. The following notes have been expanded based on information Rohan provided to the Natspec Technology Strategy Group (TSG) on 17/03/2020. This is version 1.1 of the document and was made available on 03/04/2020.

How to use this document

- **I need general IT and technology resources**.
  - We point to a number of useful resources from Jisc, Natspec and the Karten Trust
- **How is my colleges internet connectivity provided?**
  - As the method by which your college connects to the internet is vital, we suggest you understand the nature of the connection(s) you are using.
- **How are my IT systems / services provided?**
  - It is important to understand where the systems and services your college uses are provided from so that decisions can be made about prioritisation and staff instructions
- **What technologies do we use to work remotely?**
  - What technologies are available for staff communications and remote working?
- **What technologies do we use for remote learning?**
  - Consider the technologies you have available for remote learning, are they sufficient / fit for purpose?
- **I need decision making assistance.**
  - We outline some considerations to start the process.

Contents

I need general IT and technology resources.

These notes have been shared by Paul McKean (Jisc Head of FE and Skills):

- Jisc has created a dedicated Jisc web page **www.jisc.ac.uk/coronavirus** where colleges can find lots of useful information to support business continuity and learning during the current crisis.
- We also have a community of practice I would invite all participants to join **https://jisc.onlinesurveys.ac.uk/planning-for-coronavirus**

Finally, having had a number of conversations around coronavirus and technologies role. I would suggest the group/institutions start from the questions 'what are we trying to achieve?' rather than 'how can technology help?'. What I mean by this is, is the aim of the institution to remain engaged and in communication with learners/parents/carers throughout any closures? Or is the aim to deliver the full F2F (face to face) timetable online? I am sure the answer will be somewhere in between with the majority of institutions looking to the former first and foremost. If this is the case then the use of technology should focus on maintaining engagement and communication in the first instance and where appropriate supporting the continuation of teaching, learning and assessment.

Jisc resources

- Jisc Guide **'Ensuring continuity of learning during enforced absence'**
- Jisc **Planning for coronavirus webinar series**.
- **Jisc e-books for FE** (normally requires organisational subscription, at no additional cost to Jisc FE members, note that there are some **infrastructure requirements** for this service, however Jisc has now made these resources freely available until 31st July 2020 to support organisations planning for coronavirus (COVID-19) closures):
- Access **essential online content for free**
- Free **student e-textbook programme** to give university students and staff access to learning resources.
- **School's out! What this means for the #onlinepivot** advice for how to manage a move online & thoughts about how various activities consume bandwidth.
- **Online meeting survival guide**: advice for staff on how to manage online meetings.

Other sector resources

- **Natspec TechAbility Resources page**
- **Karten Network Resources page**

How is my colleges internet connectivity provided?

The first factor to consider is how your college is connected to the internet. Colleges have a range of types of internet connectivity. The main options are shown in the table below:

Type of connection	Likely speed / bandwidth	Synchronous (same speed in both directions)	Number of home workers supported?
Janet connection	100Mbit/sec – 1Gbit/sec (1000Mbit/sec)	YES	Large ~all staff can work from home.
Commercial fibre connection / leased line	Varies.	YES, but see notes on network contention below	Large to medium ~small group of staff only may connect.
Domestic grade ADSL	Maximum of ~30Mbit/sec down, 10Mbit/sec up	NO	1 or 2 people only and may not work well at all. Key staff only.
Domestic grade VDSL	Maximum of ~80Mbit/sec down / 20Mbit/sec up	NO	Small to medium, small team of vital staff only.
'fibre to the premises'	Varies.	NO	Medium, key teams only.

Janet connection

This is a fast and synchronous connection; this means that transfer speeds both 'to' and 'from' the internet are the same. Most colleges that are members of Jisc also have a Janet connection. Not all connections are 'equal' or the same, with Janet connections there is no 'network contention', meaning that you do not share your 'slice of the pipe' with anyone else. Janet connections generally operate at 100Mbit/sec or 1Gbit/sec. For comparison the best home connections are 80Mbit/sec (and they are asynchronous, this means that the speed from the internet to you may be fast, but the speed from you to the internet will be orders of magnitude lower).

With a Janet connection you will certainly be able to facilitate staff working from home, should you have the right services enabled (more below). Note that 100Mbit/sec connections or even 1Gbit/sec (1000Mbit/sec) connections will still become overwhelmed if large numbers of people are using services that take up a lot of bandwidth such as streaming video services or video conferencing services.

It can be useful to use the **Janet Netsight** service to analyse bandwidth usage, your IT team should have an account on Netsight3, if not an account can be requested. If you are consistently using half the available bandwidth it is time to consider asking for an upgrade. Note that in most cases colleges are funded for a 100mbit/sec connection. Colleges with 1Gbit/sec may have received this at no cost, for example if the regional network has been 're-procured' by Jisc, and it was possible to offer a 1Gbit/sec connection at the same cost or lower than the original 100mbit/sec connection. In some cases, where their bandwidth usage was growing colleges have opted to pay to upgrade their connection from 100Mbit/sec to 1Gbit/sec. Your Jisc account manager can assist with raising quotes for any upgrade that may be required.

In the last few days, I have been in touch with colleges who are having trouble with their connection due to a heavy use of streaming video services and other bandwidth heavy services. It is possible to 'throttle' the amount of bandwidth such services use, so that the use of the video streaming services is degraded rather than having all services (inclusive of vital comms) suffer a service degradation, or even saturation. Should this saturation point be reached services will not be reliable.

In most cases (except where very large numbers of people are attempting to use a 100mbit/sec connection) a Janet connection will have sufficient bandwidth for Colleges to continue teaching, administrative and residential activities unhindered.

Commercial fibre connection / leased line

In most cases commercial fibre 'leased line' providers will offer headline speeds such as 100mbit/sec. In reality there are often 'bandwidth shaping' tools deployed on commercial connections, or even network contention (where connections are shared between several users or organisations) that mean that 'actual' speeds are lower than 'headline' speeds.

In most cases commercial 'leased line' connections will allow sufficient bandwidth for prioritised groups of staff to work from home.

Domestic grade ADSL / VDSL / FTTP connections

ADSL

ADSL stands for asynchronous digital subscriber line; this is what most people have at home and is commonly termed 'broadband'. Asynchronous means that the speed from the internet to you may be faster, but the speed from you to the internet will be far lower. These systems use a copper line back to the exchange, and the further you are from the exchange the connection speed will drop off due to line attenuation. ADSL connections are not likely to be suitable for more than one person to connect in by any means, at any one time. It may even be the case that these connections are simply too slow for any kind of remote access to be practical. It is suggested that leaders and vital staff only should attempt remote access on such connections.

VDSL

VDSL (Very high-speed digital subscriber line) is also asynchronous, but usually gets applied to 'fibre to the cabinet' type arrangements. These are amongst the best domestic connections with speeds of up to 80Mbit/sec down and 20 Mbit/sec up.

FTTP

FTTP (fibre to the premises) is rare in domestic grade broadband installations but it is possible, although in practice speeds rarely exceed what is possible with the VDSL technology.

It may be possible for a small number of staff to work remotely using VDSL or 'fibre to the premises' connections, however performance will be poor.

Summary

Should access to 'on premises' provided services be required remotely:

- Firstly, we suggest that colleges check the type of internet connection that they have.
- If a Janet connection or commercial fibre connection / leased line is in use, remote working will likely be possible.
- If a domestic grade ADSL / VDSL or fibre to the premises type connection is in use, then we would recommend that remote working is not considered for widespread use.
- Note that if your college has remote sites, they may be served by a different type(s) of connection. This should be considered when forming your contingency plans as what is possible at your main site may not apply to remote sites that have less robust connectivity.

Your home connection

Note that the connection you are connecting in on is a significant factor:

- If you are using ADSL at home your experience will not be high quality, and remote working may not be viable.
  - If you are on ADSL and you are a long way from your local exchange the speeds you experience will be far lower due to copper line signal attenuation that gets worse with distance.
- VDSL is much better, as is FTTP, your experience will be greatly improved.
- Wireless 3G and 4G connections are possible to use, but your experience will vary with signal quality and the wider network usage.

How are my IT systems / services provided?

IT service delivery in colleges can be from both on-premises systems, from 'cloud based' systems or in many cases through a mix of both of these, this is known as 'hybrid'.

You do not (necessarily) need to connect into your college systems directly to access some services. If you are using Office 365, Google's G-suite or other 'cloud' provided services, you can usually connect to them directly.

Examples of systems and services

Table to show ***examples of systems or services*** and how they are routinely provided:

Name of system / service	Remotely hosted / cloud hosted (software as a service)	Locally hosted (from a server located at your premises)
Exchange server (email and calendaring)	Not usually.	YES
Office 365 (email, teams etc.)	YES	NO
Shared drives	Not usually.	YES
SharePoint	SharePoint Online is remotely hosted	SharePoint on-premises will be hosted on a local server
Moodle VLE	Possibly, could be provided by a third party from their servers.	Possibly, Moodle and other VLE's can be hosted locally.
Blackboard VLE	Possibly, could be provided by Blackboard from their servers.	Possibly, can be hosted on a local server.
Canvas VLE	YES	NO

Most colleges have moved their email services 'to the cloud', although some will still be using a local email server such as Microsoft Exchange. Should a college continue using Exchange it is likely that the IT team are providing access via ActiveSync to their users, so that individuals can access outlook web access (in a web browser, usually linked from a web portal) or from a mobile device such as a tablet or smartphone. If it is the case that colleges are using an on-premises email server some remote access will be required, either via mobile device active sync connections or via outlook web access (OWA). In most cases this will have already been setup by your IT team. This type of remote access can quickly and easily be setup if it is not already in place.

Office 365 and Google's G-suite have a range of other useful tools beyond email inclusive of VLE (virtual learning environments), video conferencing, intranet facilities etc. Microsoft Office 365 includes tools such as SharePoint Online, Teams, Yammer etc. Google's G-suite includes Google Docs, Google Classroom, Google Hangouts etc.

If you are already using Microsoft Office 365 or Google's G-suite then you will be aware of the facilities that these systems provide for communication and collaboration. If you have not already setup such tools it may be difficult to bring them online now.

We do not recommend that large scale IT engineering projects are undertaken unless you have a sufficiently large and skilled IT team to undertake such projects alongside 'business as usual'.

What technologies do we use to work remotely?

Note that Jisc has provided a section of our guide **'effective remote working for staff'** that can be read alongside these notes. There are a number of different remote working technologies that your college may be using to provide access to locally hosted services, such as file stores, databases and other locally hosted applications, the most common include:

VPN (Virtual Private Networks)

This is a common technology, it can be setup fairly quickly, should you have the pre-requisite software and hardware in your college. In most cases a VPN is established between client software on a remote computer and your main firewall or UTM (unified threat management) appliance. Note that there are a range of manufacturers of this equipment, inclusive of Sophos, SonicWALL, SmoothWall, WatchGuard, Fortinet etc. These appliances are generally very powerful and can handle multiple connections. It is also possible to have a software VPN configured to automatically start; Direct Access is an example of this type of technology. There is more on this point in the guide linked above, here is an excerpt:

Using VPN access: As with core systems, virtual private network (VPN) access may well be the best way to provide access to the necessary users.

Should a VPN connection be made to a privately owned computer, note that this computer may not have the same level of software and operating system security patching and antivirus protection that a corporately managed computer would. This could create a substantive risk of compromise or data loss.

In order to guard against this, a virtual desktop infrastructure (VDI) could be accessed from the personally owned computer that in effect opens a full desktop that is hosted on the organisation's servers. The user merely has a web browser window open on their computer that connects to the remotely managed virtual machine. This approach will greatly reduce the chance of information being lost or systems otherwise being compromised as corporate data will only reside on the organisation's severs and not on the privately-owned local computer.

If a corporate VPN is left running after core work has been completed that traffic will continue to traverse the corporate network. This may have an adverse impact on network bandwidth, should a large number of users do this simultaneously. Should a user continue to use their computer for non-work purposes, such as watching video streaming services then the traffic will continue to traverse the organisations network, if the VPN remains active. This traffic routing into and out of a network is known as 'tromboning'. It is suggested that users who have local control of their corporate VPN should turn it off once core work has been completed to avoid unnecessary use of resources at their home organisation.

For those users who do not have control of their corporate VPN, they may wish to limit their use of the corporate device to direct core work only. Many FE organisations use ***Direct Access****, to ensure compliance with web filtering, monitoring, reporting and alerting best practice expectation. In this situation the traffic is routed back into the corporate network on purpose, to ensure that web filtering is applied. The 'tromboning' of traffic in this case is by design, and in most cases cannot be switched off.*

Alternatively, if it is available but not already being utilised, you may consider using SharePoint sites and/or file storage areas within Microsoft Teams channels or Google G-Suite to transfer the required information for the duration of the incident. In such circumstances, it is important that such records are restored to their permanent location as soon as possible after the incident is deemed to be over.

VDI (Virtual Desktop Infrastructure)

A VDI is a more complex technology to setup from scratch as it generally requires dedicated virtualisation hardware to host the compute and storage resources required to support 'virtual machines' or virtual desktops'. Examples of VDI's are VMWare Horizon View, Citrix and Microsoft RDS (Remote Desktop Server).

If your college already has such a technology in place, it can be used to provide access to a virtual desktop from both corporately owned and managed devices such as 'domain joined' laptops and other personally owned devices in a secure way. In most cases a personally owned computer can access a VDI via a web browser, through a web portal (web site managed by the college) in order to gain access to locally held (on-premises) resources.

If you don't already have a VDI in place, it is unlikely that it will be possible to quickly set one up, due to the hardware requirements of such systems.

SSL-VPN appliance

An SSL-VPN (secure sockets layer virtual private network) appliance is another option to enable remote access. This method allows administrators to publish internal resources such as an internal web site (e.g. a database front end, OWA mail server or even file shares) via a specialist interface that can be 'published' externally to a web portal. If this technology is already in use at your college, it is likely that it is referred to by another name, possible by the name of the web portal / web site used to access it, this may be linked to as a 'staff login', area on your main college website.

Summary

If you have locally held (on-premises) systems that you want your staff to access:

- Find out what systems you have in place, and how they are to be accessed e.g. what web address is required for the 'college web portal'.
- In most cases a college domain user account will be required to access such a system. Clear instructions for accessing these systems must be provided to staff or students.

What technologies do we use for remote learning?

Consider the skills of your staff team before choosing how you might support remote learning or teach online. Note that the Jisc blog by subject specialists **Kellie Mote** and **Scott Hibberson** '**Are your staff digitally ready to communicate with learners online?**' may be useful in exploring some of these issues in more detail.

Virtual learning environments (VLE)

A number of specialist colleges have VLE's already in place. Note that as with other systems VLE's can be on-premises or can be provided from the cloud using SaaS (Software as a Service). For example, both Blackboard and Canvas provide SaaS VLE's. Moodle can be provided both on-premises or via a SaaS agreement with one of a number of specialist Moodle hosting providers. Google Classroom is a SaaS service. Microsoft Teams (another SaaS service that is part of Office 365) is increasingly being used to replace the functionality usually associated with a VLE.

In most cases the method of access to a VLE is via a web browser, to a specific web portal, these will require an organisational 'domain' login for users to gain access.

It is unlikely that a college will be able to setup a new VLE from scratch without having a substantial internal software or e-learning development team. It would be possible to spin up a SaaS (hosted) VLE quickly, but it would still take time for an e-learning technologist to assist staff to populate it. If you have an established VLE already, this can likely be used to provide some continuity of curriculum delivery. If you do not already have an established VLE, it is likely to be very difficult to provide this service in the short term at least.

Other remote learning resources

As others have created lists of remote learning technologies please see the following links:

- Natspec **TechAbility SEND specific resources**
- **ALN home school** links (thanks to Kim Lawther)
- **Home Learning Support** from the Karten Network.

I need decision making assistance.

Note that Jisc members can contact their **account manager** for further assistance and support. Note that we are experiencing a high level of enquiries and we will do what we can to get back to you as soon as possible.

Advice / guidance for specific situations

The following is for general guidance only, your college IT team are likely to be able to discuss any particular concerns around your specific situation.

My college is closed, I need basic communications only

1. Audit what systems you have already, for example:
    i. **Bulk SMS** (short message system), text messages, for example using **Janet Txt**
    ii. **Email distribution lists** for:
    a. Families
    b. Staff, or specific groups of staff
    c. Students, or specific groups of students
    iii. **Online conferencing tools** such as
    d. MS Skype / Teams
    e. Zoom
    f. GoToMeeting
    g. Google hangouts
    iv. Other **emergency or business continuity tools** such as **EverBridge** that allow staff and students to select specific methods by which they can be contacted.
2. Ensure your staff know how to access these systems, and what your expectations are for their use.

It is strongly recommended that wherever possible that you should consider using systems that you already have, rather than creating new systems at this time.

My college is closed or largely closed, our curriculum is running remotely

1. As above, audit the communications systems that you have in place already
2. Follow this by auditing the remote access technologies (see technologies used to work remotely section) that your staff team will be using to work remotely:
    i. VPN
    ii. VDI
    iii. SSL-VPN appliance
    iv. Make sure your staff know how to access these systems
3. Audit your tools for remote learning

   i. VLE's, Inc. MS Teams and Google Classroom
   ii. Online intranets (e.g. SharePoint Online)
   iii. Make sure your staff and students understand how to access these systems
4. Set expectations for how these systems are to be used
   i. What systems for what purposes?
   ii. How often will content be refreshed?
   iii. What subjects can (or should) be taught in this way?

My college is open, what technical considerations are there?

- Auditing all systems as noted above and making sure that staff and students can access them will be an important point. Whilst you may be open now, things may change in the coming days / weeks / months and this preparation may be useful
- Managing bandwidth, even on a high capacity Janet connection will be an important factor
  - Consider having your IT team monitor bandwidth use
  - The Janet **Netsight** tools are useful for those Janet connected organisations
- If bandwidth is in constraint, consider the following options:
  - Throttle high bandwidth services such as video streaming, at least on a schedule to allow vital communications and teaching and learning focussed usage during 'core hours'
  - Ask staff to use audio only conferencing, not video conferencing, audio only uses a lot less bandwidth
  - If you have a secondary connection, consider routing traffic from the residences out over this connection to leave the primary connection free for core functions
- Note that criminals are using the current emergency as a route for delivering malware, coronavirus related phishing attempts are being reported.
  - See the NCSC blog post: **NCSC issues guidance as home working increases in response to COVID-19**

Supplementary note

Jisc cannot be held responsible for the content of third-party sites linked to from this document.

All information provided here is provided on an "as is" basis and is for general information only, unless the information is part of specially contracted work, in which case the terms of the corresponding contractual agreement between us shall apply. Whilst we apply a wealth of collective knowledge and experience to ensuring the accuracy and completeness of our advice and of the information we provide, we are unable to provide any representations, warranties or guarantees, whether express or implied, as regards this advice and information. It therefore remains the responsibility of the Jisc member to ensure that they consult with all relevant roles and groups within their organisation, and take their views into consideration as appropriate, before acting upon any of the supplied advice or information.