Remote Learning Readiness Worksheet

Potential Challenges

In the event that your school is required to teach remotely, how are your users (teachers, support staff, and pupils) going to access their resources? This area describes some high level considerations and actions that can assist in ensuring remote access to resources.

Considerations and Possible Actions

1. Define your user types as this will inform the considerations and possible actions. An example of a user type includes:
   1) Staff who have a school-owned device
   2) Staff who have access to a device
   3) Staff who need to loan a device
   4) Users who have access to the internet
   5) Users who have no / limited internet provision

2. Pupil access to resources should also be broken down by age groups, for example:
   1) Senior School Pupils (Ages 14 - 18)
   2) Middle School Pupils (Ages 11 - 14)
   3) Lower School Pupils (Ages 5 - 11)

3. Determine which resources are required in the event that an issue arises. Once the different types of resources have been established, questions could include:
   1) Where are the resources stored?
   2) Does the school have shared drives?
   3) Are they accessible on the school-owned devices?
   4) Are any resources stored on web-based platforms (VLE)'
   5) Do staff have access to their software resources locally on a machine?
   6) Does the school have loan equipment that could be shared with users?

4. Even if a device can be provided, other considerations may include:
   1) Internet requirements
   2) Users may need additional peripherals to make software/resources operate as required.

5. In preparation for remote learning, users should be asked to undertake the following tasks:
   1) Carry out a speed check of their own home internet
   2) Take their laptops home and check everything works
   3) Seek IT support to mitigate issues arising in a real-world scenario

6. How do the support functions of the school continue to assist the business management needs? For example:
   - Can staff still be paid?
   - Can debtors or creditors be chased?
   - Are Admissions in the process of finalising places for the new academic year and are enrolment targets at risk?
   - Is there a need for access to the school building?
   - What happens if a server fails?
   
   Once the plan is in place for teaching staff, the school should begin by identifying areas of risk and priority in the event of an issue that impacts operations.

   Step 1. Define your user types as this will inform the considerations and possible actions. An example of a user type includes:
   1) Staff who have a school-owned device
   2) Staff who have access to a device
   3) Staff who need to loan a device
   4) Users who have access to the internet
   5) Users who have no / limited internet provision

   Step 2. Pupil access to resources should also be broken down by age groups, for example:
   1) Senior School Pupils (Ages 14 - 18)
   2) Middle School Pupils (Ages 11 - 14)
   3) Lower School Pupils (Ages 5 - 11)

   Step 3. Determine which resources are required in the event that an issue arises. Once the different types of resources have been established, questions could include:
   1) Where are the resources stored?
   2) Does the school have shared drives?
   3) Are they accessible on the school-owned devices?
   4) Are any resources stored on web-based platforms (VLE)'
   5) Do staff have access to their software resources locally on a machine?
   6) Does the school have loan equipment that could be shared with users?

   Step 4. Even if a device can be provided, other considerations may include:
   1) Internet requirements
   2) Users may need additional peripherals to make software/resources operate as required.

   Step 5. In preparation for remote learning, users should be asked to undertake the following tasks:
   1) Carry out a speed check of their own home internet
   2) Take their laptops home and check everything works
   3) Seek IT support to mitigate issues arising in a real-world scenario

   Step 1. Consider the following scenarios and their related processes:
   1) Do IT have the ability to remotely support the users? E.g. Software is available that will allow the IT team to gain remote access to a device and resolve any issues the user is experiencing. It should require the user to approve access (IT should not access without authorisation). This would require a process to be defined around IT teams having staff contact details or vice versa.
   2) Do the accounts/bursary teams have access to the finance system remotely?
   3) Are the finance and payroll systems linked or are they separate?
   4) What are the considerations or risk assessments that need to be carried out from a compliance and safeguarding perspective?
   5) By adapting the systems and working practices, is the school's data and IT network still secure?
   6) Do the proposed plans create additional risk?

   In all of the above considerations there is a need to reference the school’s crisis management plans and policies to ensure key areas have been reviewed such as safeguarding, HR, compliance, data protection, security of systems, etc.

   9ine's Security & Systems Service provides school leaders with an action plan and necessary resources for remote learning based on their specific systems, configuration, resources and device demographic. For assistance in disaster recovery planning and strategic IT management contact info@9ine.uk.com

   SUBSCRIBE TO 9NEWS FOR CONTINUED UPDATES AND RESOURCES FOR CORONAVIRUS PLANNING