In schools many staff undertake more than one role, and it may not be feasible or necessary for schools to retain in-house IT expertise. Even if you do have IT technicians or managers on-site, in an incident situation, you may feel the need to use specialist recovery services.

Data recovery specialists have the technical and logical skills and experience to recover data from computer storage devices, equipment, and/or information systems which has been lost or made inaccessible.

Services may include:

* Hard Drive / SDD Recovery
* VM Ware Recovery
* Database Recovery (inc SQL)
* Server Recovery
* NAS / SAN / RAID Recovery

If you are considering whether you will be using an external cyber incident response company you may find the NCSC advice useful:

<https://www.ncsc.gov.uk/information/cir-cyber-incident-response>

Recovery services will have access to a variety of potentially sensitive data. It is therefore vital that, if you are using an external restoration provider, you have carried out due diligence.

The provider should:

* be ICO registered
* be ISO 27001 certified as a minimum
* provide a contract and sign a non-disclosure agreement (NDA)

The UKs Cyber Resilience Centre Network run by UK Law Enforcement, funded by the Home Office, will be able to advise on accredited organisations. Tasked with *“protecting communities, promote economic growth and overall safety*”, you can get contact details for your local centre [here](https://www.brimcentre.com/network).

Files encrypted via ransomware cannot frequently be decrypted by anyone other than the attacker. However, it is worth referring to the [No More Ransom Project](https://www.nomoreransom.org/en/index.html) to check for decryption tools which might help.