

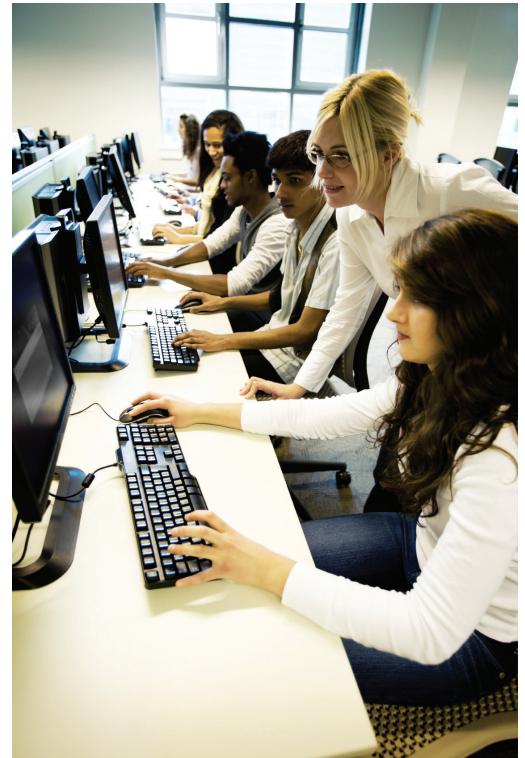


# Safe access to online educational resources

Schools and other educational providers are increasingly employing technology to enhance learning, this includes using the Internet to provide its educational practitioners with services such as remote access to school or college management systems and learner's personal records.

The Government through its ICT agency, BECTA, is promoting the safe and effective use of technology by teachers, students, schools and parents. The highly sensitive nature of the data in this environment means secure access to it is crucial. It's vitally important to know that only authorised users have access to certain resources, for example individual's records and online services such as the MIAP personal learning record.

Passwords only provide weak security, as they are easily guessed, copied or hacked, making it easy for unauthorised users to gain access to personal information. To help schools and colleges secure their data, BECTA have published a number of guidelines to help, these include the implementation of two-factor authentication to prove users are who they say they are.



## Meeting BECTA guidelines

BECTA published a report in June 2008 called 'Data Handling and Procedures in Government', which details the procedures that all public bodies, including schools and colleges should follow to maintain the security of their data. Key systems that require authentication to migrate the risk of identity theft include:

- **Government Connect**
- **SIMS**
- **ContactPoint**
- **Janet**
- **MIS remote access**
- **Online reporting tools**
- **Access to parent and/or pupil web portals**

Key focus areas within BECTA's guidelines are the provision of secure, but easy-to-use, remote access to online services for learners and parents specifically.

As the majority of school management information system (MIS) data is classified as 'IL-3 Restricted', BECTA recommends that any systems giving remote

access to this data must be protected by two-factor authentication.

Data that is held by central government, such as SIMS and ContactPoint, should only be accessed with two-factor authentication.

## Meeting BECTA guidelines with Signify's services

Signify can help you to secure your computer networks and meet BECTA's guidelines by providing a secure alternative to passwords that safely enables remote access to systems and information by delivering two-factor authentication as an on-demand hosted service. Signify have an outstanding reputation for delivering secure, reliable and flexible two-factor authentication which is quick and easy to deploy.

Two factor authentication requires two factors to validate the identity of a user, who wishes to remotely access a network or database, replacing weak and insecure passwords. By combining these two factors, you can be sure individuals are who they say they are



and are authorised to access specific educational data and information. The two factors are:

- **Something you know – a secret PIN**
- **Something you have – a token or card or mobile device that provides a unique 'one-time passcode'**

Both through compliance and a better understanding of identity management, public sector organisations are increasingly replacing insecure passwords with two-factor authentication. Signify have a lot of experience in this sector and is already the supplier of managed two-factor authentication to many educational and government bodies.

With Signify's service you get:

- **Strong network security and reliable authentication**
- **A technology that meets government and BECTA secure remote access requirements**
- **Access to all relevant government networks requiring two-factor authentication**
- **A convenient remote access solution for all educational users**
- **A choice of market leading form factors, including RSA tokens, software tokens and SMS authentication for mobile devices.**

## Why choose a managed two-factor authentication service?

Signify understands that while there is a need for all educational bodies to implement two-factor authentication in line with BECTA's guidelines, there is no standard way to do this. Authentication can be implemented by learning or local authorities and filtered down to schools and colleges or actually rolled out by schools and colleges themselves – either way has its complications and can be a squeeze on IT resources.

Signify's fully hosted managed service makes it quick and easy to implement two-factor authentication however a school or college is organised. A hosted managed service has many benefits over the in-house approach:

- **Guaranteed SLAs**
- **No need to buy, install, run and maintain any new hardware**
- **The service can be up and running in a matter of hours**
- **Scalability**
- **Provisioning of tokens**
- **No extra effort for already overstretched IT departments**
- **Fixed costs**

## About Signify

Signify helps organisations to secure their computer networks. We provide a secure alternative to passwords that safely enables remote access to systems and information by delivering two-factor authentication as an on-demand, hosted service.

**Contact us for a free trial today!**



*The Secure Authentication Service*

**info@signify.net** **www.signify.net**

**+44 (0)1223 472572**