

How Becta's "Data Handling Procedures in Government" affects your school

As schools look to use the power of the Internet, the risk of identity theft increases. Schools must mitigate this risk, and Becta has provided some useful guidance on when and how to do this.

Key applications where schools need to consider authentication technology to mitigate the risk of identity theft are:

1. remote access by staff to school networks, especially if access to management information systems is to be granted
2. online reporting to parents
3. parent and / or pupil web portals
4. ePortfolio applications
5. access to third party systems / networks (such as local authority hosted applications and data or central government systems)

Flexible working and remote access to school networks

Remote access and flexible working is becoming a standard practice as organizations take advantage of cost benefits of the internet by providing VPNs (Virtual Private Networks) for employees to access confidential data, resources and applications. Users at all levels now have the ability to access systems from home and other remote locations.

Whilst allowing remote access to school applications and resources is fast becoming a necessity in the school environment, various guidelines, best practice advice and legislative requirements exert a strong influence over what could and should be done.

Initiatives around online reporting and other applications requiring access to sensitive data are now impacting how and what school and educational stakeholders and other practitioners (potentially including parents) access these resources

The report Data Handling Procedures in Government published by Becta in June 2008 sets out in detail the procedures that all departmental and public bodies, including schools, should follow in order to maintain security of the data they hold. This includes encryption, protective labelling of sensitive data, audit and logging, operational controls for use of mobile devices – and a range of measures to ensure secure remote access.

The majority of typical school management information system (MIS) reports or data is classified by the report as 'IL3–Restricted'. Becta recommends that any systems giving remote access to such data must be protected by two-factor authentication. We provide a short introduction to that technology in the appendix below.

Online reporting to parents, parent / pupil web portals and ePortfolios

From September 2008, all maintained schools in England will be expected to start the move towards

online reporting with:

- all secondary schools providing parents with online reports by September 2010
- all primary schools meeting the requirement by September 2012.

Schools need to start preparing for online reporting and consider it alongside the secure remote access requirements. This is also an opportunity for schools to look at how they can use their existing data and systems more efficiently and effectively to share protected information.

Schools already collect and manage a range of information. The emphasis should be on maximising the use of their integrated MIS and learning technologies. As with any move to new ways of working, schools will need to review their own capability – across the whole school – to implement online reporting.

Guidance suggests that parents and learners should be provided with online access to information about:

- Attendance and behaviour (both positive and challenging)
- Progress and achievement
- Special educational needs

Remote access reporting requirements are determined by the impact level of the data being reported. Therefore, the types of information provided should be appropriate for the parent/learner.

If a school wishes parents to have remote access to IL3 data (see above) then Becta's report advises that parents will require two-factor authentication tokens and the use of password-protected files to enable secure communication between the school and themselves.

In addition to online reporting, many other web-based portals and applications are being considered by schools, including for example pupil ePortfolios. For each of these applications best practice suggests that

a school should consider the impact level of the content being made available by the portal and what level of authentication security is required.

An introduction to Two-factor authentication (2FA)

Two-factor authentication is a well established technology that is implemented throughout government and enterprises. Its implementation is usually driven by

- a response to some form of regulatory guidance or mandatory compliance instruction, such as FSA rules in banking HIPPA rules in healthcare, CoCo (Code of Connection) rules in UK government and arguably Becta's advice in the circumstances outlined above
- the application of best practice security guidelines

The need for 2FA is driven by the fact that the standard password invented more than 50 years ago is now the weakest link in any IT network. It is easily guessed, hacked or stolen.

"Strong password" policies that force more complex passwords and regular password changes do not mitigate the risk of most hacking techniques (social engineering, shoulder surfing, key logging, Trojans etc) and so their impact is normally limited to vastly increasing help desk calls as users forget their passwords. 2FA by contrast should result in a significant reduction in help desk calls.

Virtually everybody uses a form of 2FA today when they use a bank card to withdraw cash. 2FA demands that you prove your identity using a "something that you know", such as your 4 digit PIN, and a "something that you have", such as your bank card. For network and application access the something that you have is known as a token - the token provides a onetime password which is used in conjunction with a PIN number.

Some things to consider when implementing 2FA

A good authentication system gives you the flexibility to provide the users with the most appropriate form

of token. Tokens can be small hardware devices with a button and screen, they can be software based, smart card based and can even be implemented on mobile phones using SMS technology. User acceptance is a key issue in 2FA implementation and the right choice of token can ensure almost universal acceptance from end users whilst a bad choice of token can severely hinder usage. Choice is key.

Schools are also going to need flexibility when it comes to integration. Code of Connection doesn't solely revolve around authentication. Firewalls and Intrusion prevention, detection scanning and anti virus tools will be part of the package and so simple integration of your 2FA system within your network and applications should be high on your agenda.

Finally ease of use of the 2FA management system must be paramount. Wide functionality, automation of common tasks and reporting, and an intuitive interface are musts.





CryptoCard Certified Partner



Tel North: 0151 2031400 Tel South: 0118 9071600
Email: Info@castleforce.com Web: www.castleforce.com

CRYPTOCARD
Secure Your World.