

Becrypt for Education

Protecting sensitive child and parent data with government approved data security products

Becrypt Data Security for Education

Protecting sensitive data, particularly child and parent data, has always been important for schools. Under the Data Protection Act 1998, educational institutions have a legal obligation to protect personal and sensitive information about their pupils, students and staff members. Organisations losing personal data risk bad publicity and loss of reputation, as well as possible fines imposed by the Information Commissioner's Office (ICO) for non-compliance with data protection legislation.

All your security issues covered by one supplier

Schools need to be able to protect information effectively and transparently to the end user. The ICO recommends that sensitive information held on desktop and laptop computers should be encrypted, as well as data that is held and transported on CDs/DVDs and USB devices, and data that is accessed from outside via VPN or other secure network link. Desktops and laptops also need to be protected from the introduction of viruses and other malware that can accidentally infect the network through the use of unmanaged USB devices, such as those brought in from home.

Whole Disk Encryption – (or Full Disk Encryption) is the method recommended by BECTA for protecting data held on desktop and laptop PCs. By encrypting the entire computer, the user does not need to think about what files should be encrypted because it happens automatically in the background.

Secure Remote Access – For people that need to be able to work from home occasionally, devices are available that can provide secure remote access to the school network from a home or other unmanaged computer.

Port control – also known as end point security, manages the devices that are attached to the network, like USB sticks or other USB drivers. This enables the school to stipulate that only approved USB devices can be plugged into its desktops and laptops, and to monitor what data is downloaded to those devices. This protects the computer and the network from contamination, it also guards against data leakage.

File encryption

Where data needs to be shared with authorised third parties, like Local Authorities, police and social services, data saved to a CD or DVD needs to be encrypted and password protected to comply with the Government's Data Handling guidelines.

Becrypt's special Data Security Starter Pack for Schools

In order to comply with the intent of Data Handling Procedures in Government, organisations, including educational institutions, must take a comprehensive approach to data security. On its own encryption is not enough to secure data. Other important measures include identification, authentication, authorisation, accountability and audit, all of which are explained in detail in the Government's good practice guides.

To get you up and running with a bundle of comprehensive security products that will help you to meet the Data Handling guidelines Becrypt has put together a starter pack especially designed for schools.

The Starter Pack includes:

- 3 DISK Protect full disk encryption licenses
- 3 Connect Protect port control/end point security licenses
- 1 Becrypt Trusted Client for secure remote access
- 1 Media Client to protect data saved to CDs/DVDs for sharing with authorised third parties
- Maintenance for first year included

DISK Protect

Becrypt DISK Protect is Becrypt's Data at Rest solution to secure a school's data, whether on desktops or laptop PCs. It gives complete peace of mind that data held on laptops and PCs is fully protected in the event of loss or theft. The hard drive is transparently encrypted, with no impact on performance. Using strong user authentication, unauthorised access to data is prevented.

Benefits of DISK Protect include:

- Deployment with minimal user interaction and with no disruption to school activities
- Easy to use – users do not need to remember to encrypt files, it happens automatically in the background
- Users do not need to remember multiple passwords
- Data is always protected even when PC goes into hibernation
- Data on encrypted machines is indecipherable even the PC is reassigned or decommissioned
- Multiple users can be added to a single PC allow secure sharing of resources

Connect Protect

Connect Protect is Becrypt's end point control solution that protects schools against data leakage, by preventing unauthorised access to and use of external devices and by providing centrally managed audit trails for all connection events. Connect Protect controls the use of all 'plug and play' devices, USB sticks and other removable media, enabling schools to enforce a usage policy. It prevents unauthorised devices from connecting to the network, or it can restrict their use to approved devices only.

Benefits of Connect Protect include:

- Straightforward and fast to deploy as only centrally issued, approved devices maybe used – enforces Information Assurance policy
- Easy to manage – no additional training is required for

the administrator

- Usage of devices easily tracked with full audit reports
- Data copying histories are easy to track and trace if investigations are required
- Email alerts for administrator mean that they are freed from the task of regularly manually checking on systems and devices used
- Challenge/Response allows temporary access to reset passwords

Trusted Client

Trusted Client is Becrypt's innovative secure remote access solution. Trusted Client significantly reduces the risk of data loss and data leakage while providing a low-cost, secure access to the school's network so that staff can work safely from any location. Trusted Client transforms an unmanaged computer (like a home PC) into a secure access point allowing staff to work securely from a PC that has a network connection. Simply by inserting the Trusted Client device into a USB port and re-booting, a secure environment is launched, providing user interface, web browser, and email access and standalone applications. Only the PC screen, keyboard, mouse, memory and processor are used. The hard drive is bypassed so that no data can be leaked and no malware can infect the network. Staff no longer needs to be issued with laptops for occasional remote working.

Benefits of Trusted Client include:

- Flexible and mobile working capabilities provide staff with a better work/life balance
- Absolutely no transference of data significantly reduces the risk of data loss or data leakage
- The device and any data saved is securely protected from unauthorised access
- Strong user authentication
- Extremely cost effective with low hardware costs
- Out of the box integration with standard browsers and therefore familiar look and feel makes it popular with staff
- Central management of devices means that if one is lost or stolen it can be repudiated immediately or a user's rights revoked.

Media Client

Becrypt Media client is a software based file encryption solution that protects data whilst in transit or on removable media such as CDs, DVDs or USB devices. Media Client offers a simple and easy way to protect data in transit. It resides on any removable device with a zero footprint allowing an authorised recipient to access protected data without needing to install software. In the event of the password being forgotten or unknown, data remains totally secure, the files can be seen,

but not the filenames or extensions revealing the data type.

Benefits of Media Client include:

- Simple and easy to use allowing non-technical users to easily secure data
- Event log generates automatic audit trail showing the data being exported
- Filenames and extensions are hidden from unauthorised users for additional confidentiality
- Zero footprint design and extractor application means that data can be encrypted quickly by the sender and read by the recipient (with password/phasephrase) with no need to have Becrypt software installed
- Data recovery facility using certificates enables straightforward access to data by the administrator should a password be forgotten or unknown
- Built in integrity/verification facility protects the contents from being tampered with while in transit.
- Files written to CDs/DVDs/USB media from within Media Client so no need for additional CD/DVD burning software

About Becrypt

Becrypt is the UK market leader of data security, media encryption, disk encryption software and remote access products that can be configured to the individual needs of your organisation. Our data security products protect the data and information on desktops, laptops, USB sticks, mobile devices and removable media such as CDs. Some of the most secure organisations in the world rely on Becrypt disk encryption software to protect their data. We work with global corporates and public sector organisations such as the UK Government, Ministry of Defence, Local Authorities and Local Education Authorities on many data security development projects. Our disk encryption software, media encryption and data security products are certified by the leading security assurance schemes, including CESG Assisted Products Scheme (CAPS), CCT Mark, Defence INFOSEC Procurement Co-Operation Group (DIPCOG) and the Federal Information Processing Standard (FIPS).

Who uses Becrypt

Ministry of Defence, Central Government Departments, Local Authorities and most of the UK police forces use Becrypt data security products.

Certifications

Included in our suite our products are certified and accredited by:



For more information please call 0845 838 2050 or +44 (0) 20 3145 1050, or visit www.becrypt.com

Becrypt Limited, 90 Long Acre, Covent Garden, London WC2E 9RA. www.becrypt.com info@becrypt.com

Becrypt is a leading supplier of innovative Information Assurance solutions and services with operations in the UK and US. Becrypt provides secure, feature rich, out of the box products suitable for all industry sectors, and is the largest supplier of encryption technology to the UK Government, Ministry of Defence and UK Police.

© Copyright 2010 by Becrypt Limited. All Rights Reserved. The Becrypt logo and trademarks are owned by Becrypt Limited. No material may be reproduced for any purpose, private or commercial, without prior written permission from Becrypt Limited.