



# STARS Modern Thinking For Education

## HOW DO I? Data Protection Act & Security

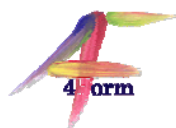
This guide describes how the Data Protection Act applies to STARS and general security issues that you should be aware of when using STARS.

### ***Terms Used***

Term Used	Description
ACTION	This details the steps you must take when following this guide.
Administrator	A user with ADMIN or SUPER USER role access to STARS.
Antivirus	Software that scans your computer and email for malicious programs.
DPA	Data Protection Act.
Encryption	A process of adding security to data so that it cannot be read without having the correct key to unencrypt the data.
Firewall	A software program that stops unauthorised connections from being made from or to your computer.
Login	The generic term for a username/password combination or the process of entering username/password to gain access to STARS.
Online Server	A STARS installation hosted by FourForm. Access to these systems is available from anywhere via an Internet connected computer.
Push/Pull	A mechanism for requesting or sending information to or from a FourForm server.
Role	Functionality within STARS is granted by allocating each user to a role. Roles are READ ONLY, STANDARD and ADMIN. A fourth role exists for standalone servers called SUPER USER. This role gives access to server hardware administration functions. Depending upon your login role, menu options are displayed or hidden.
Standalone Server	A STARS installation where a server is installed on site. Access to these systems is only available from the site network and not via the Internet.
User/Username	This is a person who has access to STARS or the name that they use to log into STARS.



- Never give out your username or password to STARS.
- Never leave your computer logged in and unattended when using STARS.
- Check your network administrator has secured your wired and wireless networks.
- Never store any uniquely identifiable information on your computer unless you have encrypted it and access is via a login that only you are aware of.
- Keep your antivirus and firewall up to date.



## How Does Data Protection Apply To STARS?

In general, the Data Protection Act (DPA) is designed to make sure that any data that is stored is only used for the purpose that was set out when the data itself was collected. STARS is available on two platforms, the legacy standalone server (no longer available to purchase) and the online server (legacy systems can migrate to this platform), the details on how the DPA applies to both systems is explained below.

### Legacy Standalone Servers:

For legacy standalone servers, there is no data protection requirement from FourForm as the data and server are both located on your premises. FourForm do not have access to your system; we cannot initiate a connection to your server via the Internet or any other mechanism. Any information exchanged from your server to one of our servers is via a “Push” or “Pull”. For example, your server may connect to ours to request new packages for download (“Pull”) or send information to our servers to report problems with your system (“Push”). FourForm can initiate neither “Push” nor “Pull” on your server.

Access to your standalone server is available from your network; FourForm has no control over who accesses your network or from where access is permitted. At most sites, access should be restricted to connections made from within your own network. Again, FourForm have no control over this and it is a configuration issue for your network administrator to ensure that the correct firewall and exemptions are in place.

To login to your standalone server you will have been informed of the IP address to use, this will be an address on your network range in the format “http://nnn.nnn.nnn.nnn” where “nnn” is any number between 0 and 255.

### Online Servers:

For online STARS systems (where you can access your system from any Internet connected PC) FourForm hosts your system on one of our servers. In this respect FourForm acts a data storage facility. We do not use any of your information for any purpose other than to support your STARS system. Data is not sold, transferred or exchanged with any third party. During support calls, it may be necessary to log into your system to view screens. In these instances permission will be requested to log into your system using our own user account. These sessions are subject to the same audit logging as for all other STARS accounts. See the User Maintenance Options HDI? Guide for more information on how audit trails are recorded within STARS.

To login to your online server you will have been issued a unique address for your school in the format “http://yourschool.fourform.com”. Entering this address will take you to the validation page for your school where you can click on the link to continue to the secure login page. From this point, all information exchanged between your browser and the online server will be encrypted.



### Online System Data Transmission:

Data transmitted to and from the online STARS system is encrypted to ensure that the information cannot be intercepted between the central server and your local computer.

- Check that the address you are using when logged in begins “HTTPS” – the “S” indicates “secure” and the traffic is encrypted.
- Check that the padlock symbol is displayed in your web browser. Depending upon your browser type, this will likely be either next to the web address or in the bottom status bar.
- Ensure that the “Secured By GeoTrust” logo is displayed near the end of each page (click on the logo to verify the details of the certificate).

### GeoTrust Encryption

STARS uses GeoTrust SSL server security to encrypt the data exchanged between your browser and the online STARS server. The GeoTrust logo (shown below) is displayed near the bottom of every page on the online STARS system. This logo is generated as each page is requested, a date and time-stamp is shown at the bottom of the logo.



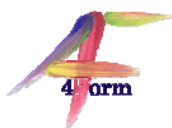
You can click on the logo to see more information on the certificate issued by GeoTrust for STARS. More information is available on SSL encryption and the GeoTrust certificates from the GeoTrust website at <http://geotrust.com>

### Message Specific DPA Information:

Message information is automatically downloaded overnight from the FourForm central server to the online servers and to the legacy standalone servers. Both systems initiate a “Pull” of data from the FourForm server and install it as a message on their own systems. No information (apart from information needed by the transmission application to determine if the transfer should be authorised and if the transfer has been successful) is transmitted back to the FourForm server.

### Wireless And VPN Access:

Wireless technology is becoming more prevalent to allow access to home and site networks. Although this allows the freedom to connect without wires, it also allows potential for unauthorised access if the wireless settings are not configured correctly. Check with your network administrator that any wireless installation is secure. This also applies to Virtual Private Network (VPN) configurations that allow external connections to your local network. Data transmitted via an unsecured wireless network may be intercepted and viewed by unauthorised persons.



**General Good Practice:**

When accessing and saving pupil information to the computer you are using to connect to STARS, you should be aware of your own data protection policy. In general, it's best not to save any information on your local computer as this presents a risk of data loss or unauthorised access. Try to access the data online wherever possible and if you need to store data remotely then try to make sure it is encrypted or password protected.

Access to most computers is via a password. This is the same for STARS; never give out your username or password. Each person who logs in to STARS should have their own username and password. If you think your password has been compromised then ask an administrator to reset it straight away. As soon as the administrator has reset your password, log back in and choose another password that only you know.

Ensure that you use strong antivirus software and keep it up to date. There are a number of basic, free antivirus programs available for personal use and site licensable programs that cover multiple computer installations: Check you have one installed. Keep your firewall turned on and ensure the exceptions list is monitored.

**More Information On The DPA:**

More information about the Data Protection Act can be found at The Commissioner's Office website: <http://www.ico.gov.uk/>

