Glow Security

This document gives an overview of the security in place for Glow users on the current Glow environment, which will be available until September 2012.

We take the security of Glow very seriously and by design Glow provides a trusted and safe environment for pupils, teachers and parents. During the development of Glow we engaged a specialist computer security consultancy who using CLAS registered consultants ensured secure coding standards, risk assessed detailed systems designs and assisted in ensuring the service took appropriate safe guards, following ISO 27001 and CESG security standards, to protect Glow from attack. Since its' launch in 2007 there have been no security incidents at a national level.

Single Sign-on

Glow allows users to sign on once (single sign-on, using their username and password) and then access a range of services either delivered by Glow or carefully chosen third party suppliers providing nationally procured education content without having to logon again. The user accounts are securely stored within Microsoft Active Directory[1] and Glow services are then further protected by Oracle CoreID Identity management[2] or by shibboleth[3]. This means that only authorised users can access Glow. The National Directory provides an index of all users, but who you can see and what details you see when you log in to this area depends on the parent, pupil or teachers 'role'. Permissions granted to roles are hierarchical: national; local authority and establishment. School administration staff cannot grant local authority or national permissions; Local authority staff cannot grant national permissions. A parent's view will be different from their child's, and different from a teacher's.

[1] http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory.aspx
[2] http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html
[3] http://shibboleth.internet2.edu/

Usernames

All user accounts for Glow need to be unique. When you get a glow generated username it will be in the form gw08smythshawn2
Gw (for glow generated) 08 (Year of creation) smyth (your surname) shawn (your given name) 2 (an additional number may be generated to ensure uniqueness).

Physical Hosting

The Glow data centre is hosted within a secure Tier 1 co-location facility ensuring the high possible integrity of network, power and physical access.

SSL Encryption

For protection all Glow pages (including all Glow Mail pages) are secured using SSL certificate with 128-bit encryption[4]. This certificate is used to encrypt data and will also verify that the site you have a connection to is the genuine website. All the data that is uploaded to Glow and downloaded from Glow is encrypted using the SSL certificate.

SFT

Glow also contains an additional Secure File Transfer (SFT) program that can be used to transfer with additional security of limiting access to the file, limiting the time the file is available and security on access to the service.

Glow Mail

Glow Mail contains the security above along with the standard security that you will get with most mail solutions and still has the protection of Microsoft Active Directory and Oracle CoreID. Like the rest of Glow all web pages are presented using a public key 2048-bit certificate and then encrypted using 128-bit ciphers. When using rich clients to access Glow Mail, only the secure versions of the protocols are supported.

[4] http://www.verisign.co.uk/ssl/ssl-information-center/what-is-ssl/index.html?sl=t49600343700000018

Security and Security Testing

In depth penetration testing of the Glow perimeter network security is carried out by a CLAS-certified third party at regular intervals. This ensures that Glow is consistently checked against all current best practice. The last test was carried out in November 2011. No critical issues were identified and no issues were discovered that put any of the systems at imminent risk of compromise.

The data within the Glow Data centres are also protected by perimeter network security devices, such as: firewalls; virus detection software; and malware detection to protect against external attacks.