Security and Good Practice in Glow

Creating Strong Passwords

- Your password should be difficult for other people to guess, but easy for you to remember. Using a group of words or a phrase, as well as using symbols, spaces and capital letters, can make passwords stronger. Below are a few examples of passwords from Glow Connect (a Glow support site):
    - ***small grey mouse*** is an example of a very strong password, as, despite appearing basic, it is not easily guessed
    - ***D11giTal%$*** is very strong, as, despite being shorter, it uses different character types
    - Conversely, ***Pa$$word1*** is actually a weak password, as it is common and easy to guess, despite appearing complex.
- When setting a password in Glow, there is a minimum requirement for password strength; as you type a new password, a rating (ranging from "Very weak" to "Very strong") will appear to reflect this. The password is rated on a number of factors such as how common the password is, how long it is and the use of different types of characters.

Secure Use of Glow

- Don't let others access Glow using your account, including any accounts you have access to which have administrative privileges
- Don't access Glow with someone else's account, including accounts with administrative privileges that you have not been authorised to use
- Be careful if using Glow in a public space and be aware of who can see what you are doing, especially if you are accessing information that should not be shared with, or seen by, others around you
- Where pupils and staff are working away from school premises, there should be a process in place for users to be able to securely reset (or request a reset of) their passwords or confirm their user names.

Using Accounts with Administrative Privileges

- By default, teachers can reset pupils' passwords in Glow. It is also possible to give other staff "Password Admin" rights to support this. As well as pupil accounts, Password Admin rights also allow resetting of other staff accounts' passwords
- Establishments can have more than one administrative account (or normal account with administrative privileges such as Password Admin rights) assigned to allow for flexibility and additional support in managing others' passwords.

Protecting Access to Accounts

- Always keep your Glow password to yourself – don't share it with anyone else. Similarly, user names and passwords should not be posted publicly on social media
- Always sign out of Glow when you are no longer using it. When you sign out of Glow, you may also be prompted to sign out of connected services you have accessed through Glow, such as G Suite. You should sign out of these as well
- Staff with a Glow account should set up a password recovery email address, which will allow them to reset their own password should they forget their login details. This password recovery email address should not be their Glow email address, as they will not be able to access this in the event that they cannot log in to their Glow account.

Data Security

- Be mindful that any information you share may then be beyond your control; as such, be aware of sharing settings, who you specifically want to share the information with, and whether it needs to be shared this way
- Do not post any content that you would not want other learners, teachers, or parents to see. Similarly, don't post content that you don't have permission to use
- Remember that only information related to the delivery of education should be created, stored and shared in Glow. Other systems (such as SEEMiS) are more appropriate for sensitive and specific information. For more guidance on this, see the Digital Learning Team's *Guidance on Data Sharing in Glow* document at: https://blogs.glowscotland.org.uk/ab/public/sali/uploads/sites/1389/2020/03/05155952/Guidance-on-Data-Sharing-in-Glow.pdf