Password Policy for Staff and Students

POLICY STATEMENT:

With the rise of external influence trying to gain access to EKC systems via social engineering attacks (Phishing/Spam/Malware) and the responsibility of the group to protect staff and student data under GDPR regulations there is a need to ensure we are managing access to all systems.

The aim of this policy is to ensure a standard exists across all group systems for complexity and change process and frequency of all passwords and to identify when a password needs to be changed due to compromise or a staff member leaving EKC employment.

POLICY DETAIL:

There are a number of systems that require passwords. The majority of these are managed by EKC Group Active Directory (AD) and when changed synchronise across these systems. For these systems the current rules are in place.

- Passwords expire if not changed after 366 days with the user reminded 14 days before this happens
- Password compromise – if passwords could have been compromised, they must be changed immediately.
- Password Sharing – user passwords must not be shared, any indication this has happen will force a password change.
- Passwords must never be reused – you must never set your work password and for example your Facebook password to the same thing, or even your work computer password and a separate work-related system.
- All passwords must comply with the complexity settings agreed and enforced by the systems. This is set as.
    - Must be at least 12 characters long
    - For staff it must include one Uppercase/number/special character
    - As an inclusive establishment we recognise that there are some staff and students with special needs that may find this requirement challenging, they will be managed on a case-by-case basis and where necessary issued alternative methods such as YubiKey to login
- A guide to creating a strong password will be available to all staff members on the EKC Intranet which they are expected to follow when creating a password.
- Multifactor Authentication (MFA) must be enabled wherever possible
- Systems or Sites which are Single Sign On are preferred when selecting new system.
- Password-less logins are recommended where available (FIDO2/WebAuthn or Biometirc)

Where possible systems are linked to the central identity service Active Directory (AD) and external cloud-based systems will be linked to Azure login and make use of the security and MFA checks of that. Internal systems if accessible externally will utilise the protection of Azure Web application proxy and similar technology to protect and enforce MFA.

For systems where passwords are not managed by AD, individual users are granted access on an ad-hoc basis depending on job role and requirements. These systems will allow passwords based on the settings configured within that software, however reasonable effort needs to be made to synchronise centrally by AD wherever possible.

Passwords for external sites, like the DFE and other Government sites also need to follow these rules as do company social media accounts.

To enable the smooth day-to-day access to systems for all staff and students there exists the ability for staff members', dependant on their job role, to reset passwords. This ability is currently set as,

- Teaching staff can reset student passwords, this is completed via a link provided on the Digital page of the intranet and will reset the student password to the default format detailed on the reset web page.
- Line managers can reset user account passwords of staff that they are responsible for. This will reset the staff members' password, emailing the manager with the new password as well as sending an email to the staff member.

All password resets, either for staff or students, must have permission from them or only be used to grant them access to their own accounts. Their identity must be confirmed to ensure you are resetting the right account. Password resetting must not be used to access any user accounts for the purpose of gaining access to stored data, any misuse of this system will be subject to disciplinary action being taken.

An account will be locked out for seven minutes if ten incorrect password attempts are made.

Leaver's passwords will be reset, and access removed as soon as it is no longer required. For all systems synchronised by AD this will automatically happen once they are registered as leaving the company in the HR system and the last day of employment has passed. The account will automatically be removed and archived once 14 days have passed, any access needed to data in these archived accounts will need to be requested by People Services to the Digital Department.

For all systems internal and external not synchronised by AD then it is up to the line manager to ensure access is removed as soon as it is no longer required. Failure to do so could lead to unauthorised data access and the need to notify the Information Commissioners Office under GDPR regulation.

Multi-Factor Authentication (MFA) must be used where available and will be enforced as a standard in future. MFA is mandatory when logging in offsite.

When logging into a site like office 365 you will need your username, password and to have your trusted device nearby to receive a 6-digit code. This could be a text message to a mobile or voicemail to a landline or use of the Microsoft Authenticator App or some other device in the future.

Any indicators or compromised accounts will force MFA confirmation and password change.

Password Managers are recommended to make it easier to have different passwords for different systems. EKC Group is currently investigating enterprise class password managers, to allow storage of work-related passwords in a secure way for sites like the DFE and Government sites.

Staff and Students are recommended to enable MFA for other sites in their personal life as well.
General password manager advice from the National Cyber Security Centre
https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

Related Policies
IT Acceptable Use and Social Media
IT Physical Access to Sensitive Equipment
IT Technology Device Commissioning
IT Technology Special Access Request
IT User Creation and Removal Process