St Anne’s School and Sixth Form College

Password Policy

Introduction

St Anne’s School and Sixth Form College and Residence will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another’s files, without permission (or as allowed for monitoring purposes within the school’s policies)
- Access to personal data is securely controlled in line with the school’s personal data policy
- A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email, SIMs and Education City.

Responsibilities

The management of the password security policy will be the responsibility of:

overall	Lesley Davies
network	theonepoint, Sara Tharratt
BSquared	Debbie Johnson
School Pod	Kay O’Neill, Debbie Johnson, Sara Tharratt, Shiona Nicholson
Sims	Debbie Johnson, Sara Tharratt, Shiona Nicholson
Email	Debbie Johnson, Kay O’Neill,
ERover	Taff Bowles, Kay O’Neill

Updated February 2018

Education City, IXL and Espresso Coding	Sharron O'Keefe
Twitter	Sharron O'Keefe, Rachel Pearson, Kay O'Neill

All users (adults and children (where applicable)) will have responsibility for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users and replacement passwords for existing users will be allocated by theonepoint (network), Sara Tharratt (SIMs and network) and Sharron O'Keefe (Education City, IXL and Espresso Coding).

Any changes carried out must be logged in the password security file using the school format and will be checked regularly by Mrs Lesley Davis.

All users (staff) will be compelled, at initial log on, to change their passwords on a set time basis.

Training and Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password policy:

- At induction and yearly staff meetings on online safety
- Through the school's Online Safety Policy and password security policy
- Through the Acceptable Use Agreement

Children will be made aware through

- Computing lessons and/or online safety lessons
- Through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Computer Committee. All users (staff and one cohort of students) will be provided with a username and password by theonepoint and Sara Tharatt (network, SIMs), Kay O'Neill (e-mail) and Sharron O'Keefe (Education City, IXL and Espresso Coding) who will keep an up to date record of users and their usernames. Users will be compelled to change their password at a set time for the network logon (staff and one student cohort).

The following rules apply to the use of passwords:

- Passwords must be changed on a set time basis (see earlier section under Responsibilities)
- The last three passwords cannot be re-used
- Must not include proper names
- The account should be “locked out” following five successive incorrect log-on attempts
- Temporary passwords eg used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen
- Requests for password changes should be authenticated by (the responsible person as noted above) to ensure that the new password can only be passed to the genuine user

The “administrator” passwords for the school ICT systems, used by theonepoint will be available to Lesley Davis and will be kept in a secure place.

Auditing/Reporting/Monitoring/Review

The responsible person, Lesley Davis, will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy In the event of a serious security incident

The police may request and will be allowed access to passwords used for encryption. (In Maintained schools) Local Authority Auditors also have the right of access to passwords for audit investigation purposes. User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by Mrs Lesley Davis and the online safety Governor on a termly basis. This policy will be annually reviewed in response to changes in guidance and evidence gained from the logs.

Review

A review of the policy will be undertaken in line with the policy review timetable and any amendments or updates will be reported to the Governing Body.

Any new legislation or directives will be incorporated into the policy as necessary