E-Safety Suite of Policies

Passwords and Password Security 2016/17

The key principles of our policy on passwords and password security are:

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- All users should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT Support Team when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a student or colleague your password
- If you aware of a breach of security with your password or account inform the ICT Support Team immediately
- Passwords must contain a minimum of eight characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols where appropriate
- If you think your password may have been compromised or someone else has become aware of your password report this to your ICT Support Team

Password Security

- Password security is essential for all users, particularly as they are able to access and use student data. Users are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.
- All users read and sign an Acceptable Use Agreement/Code of Conduct to demonstrate that they have understood the school's E-Safety Policy and Data Security
- All systems provided by the school, have unique passwords for all users.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our school, all ICT password policies are the responsibility of the ICT Support Team and all staff and students are expected to comply with the policies at all times

Zombie Accounts

- Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- We will:
  - Ensure that a user account is disabled once the member of the school has left
  - Take prompt action on disabling accounts to prevent unauthorized access
  - Regularly change generic passwords to avoid unauthorized access

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your line manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Safe Use of Images
Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher

Publishing Student's Images and Work
On a student's entry to the school, all parents/carers will be asked to give permission to use their student's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the student attends this school unless there is a change in the student's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
Parents or carers may withdraw permission, in writing, at any time. If there is a parental 'no consent', then this is deemed to over-ride a 'consent give' parental request
Students' names may be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.
Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images/ films of students are stored securely on the school's network
- Rights of access to this material are restricted to the teaching and associate staff and students within the confines of the school network or other online school resource