

# Conyers School

*Perseverando  
Through perseverance*

---

---

## DIGITAL DATA SECURITY POLICY & GUIDANCE

---

---

Updated: June 2020

Origin: Director of School Systems

Introduction:

### ***Accessing Sensitive Data***

Sensitive digital data refers to any information used at school which is confidential, delicate or private. It relates to administrative and student data in every respect, in terms of academic performance or personally sensitive data relating to individual students. In compliance with the Data Protection Act, all personal data must be kept secure, transmitted and used appropriately. When using sensitive data the following guidance should be adhered to:-

- Data should never be left accessible on a school computer (e.g. SIMS.net left open unattended) and never transferred beyond the control of Conyers (e.g. not emailed or sent to external parties).
- Stored and used only on authorised platforms:
  - Microsoft SharePoint (ConyersNet)
  - G-Suite (Formerly Google Apps)
  - SIMS.net
  - School computers or school laptops/tablets
  - Secure remote connections (e.g. Stockton Remote Access).
- Data should be shared only with appropriate school parties.
- Sensitive and personal data should never be sent or transferred via Personal Email, USB storage devices or personal online storage. To avoid data being sent inadvertently to the wrong recipient, it is recommended that sensitive data is never emailed in any capacity. Instead one of the following solutions should be used:
  - Stored in a private folder (e.g. Admin Shared or Staff Shared) and the recipient informed of the location.
  - Uploaded to a private / staff area on Microsoft SharePoint.
  - Shared via Conyers Cloud with the relevant recipients; paying close attention to verify the recipient before activating the share.
  - Kept in its original location (e.g. SIMS) and accessed remotely using a secure connection (Executive Team only).
- Email is not a secure medium and therefore should never be used to send extremely sensitive, emotional or personal data about students.

Policy:

### ***School E-Mail on Mobile / Tablet Devices***

Staff can access their school email on a personal mobile, tablet or portable device (e.g. laptops, netbooks etc.) Staff are required to adhere to the following procedure when doing so:-

- The device being used must be configured to access email remotely (i.e. not actually store email on the device).
- The device is equipped with a lock, pin or passcode system, preventing access to email if the device is left unattended, lost or stolen.
- The device has location tracking and remote erasing facilities and these are activated. In the event of device loss or theft, it must be remotely erased to prevent access to e-mail.
- If a device has multiple e-mail accounts configured, any correspondence relating to school should be done so through the school email account.
- Personal e-mail accounts should never be used for school correspondence.

Direction and advice to device compliance can be sought from the Director of School Systems.

# Conyers School

*Perseverando  
Through perseverance*

## **Digitally Communicating with Students**

When communicating with students using digital technologies, the following policy should be adhered to:-

- Only use school communication systems (e.g. school email) to communicate with students. Only school addresses can be shared with students to communicate.
- Staff must never give out personal information (e.g. mobile phone number) to students.
- All communications, both to and from students must be saved and never deleted.
- Any initiation of communications to a student should be done purely for school related matters.
- If using personal devices to contact students (e.g. a mobile phone), staff should withhold or mask their phone number when doing so.
- Staff should not use social media to communicate with students, befriend them or interact with them in any way.
- Any communications received from students via social media should be retained, printed and the Director of IT Services or a member of the Executive team notified immediately. Under no circumstances should a member of staff reply to such communications.

## **Social Media & Gaming Use**

Many staff use social media such as (but not exclusively) Facebook, Twitter, YouTube etc. When using these systems, staff should take note of the following guidance:-

- Personal social media accounts should never be used to communicate, befriend or interact with students.
- The digital communications guidance above should be followed when receiving messages from students.
- Staff should not discuss, advertise or comment upon school matters via social media. Staff should never bring the school into disrepute in any way through public platforms / social media.
- Student data, photos, videos and other multimedia of the school should never be published on personal social media.
- Staff should never initiate or participate in any form of online gaming or interactive sites with students.
- When students leave Conyers, staff should never accept 'requests for friendship' on social media for at least one year. Staff should also be aware of the 'friends of friends' principle when befriendng ex-pupils, in the event that they have current Conyers students within their social network, who may then be able subsequently access personal online activity.
- Staff should ensure that privacy settings are sufficiently robust, to prevent any issues with student access to their personal online presence.
- Should staff use social media for education (e.g. Twitter, Facebook Groups, YouTube channels etc.), this should be done so in a transparent and public manner; under the strict direction of the Director of School Systems.

Staff should always seek clarification if they are not sure before proceeding to use social media in any relation to Conyers School.

How it will be monitored: checking IT systems	By whom: Director of School Systems
--	--

Review Date: Annually, June	Review Assigned to: Conyers LGB Care, Support & Guidance Committee
--------------------------------	--