DATA PROTECTION: SAFEGUARDING PERSONAL DATA

Data Protection laws introduced and updated in 2018 emphasis safeguarding personal and sensitive data. These include rules for aspects of how data is collected, stored, shared, used and disposed of.

Individuals also now have more control over how their personal data is processed and sensitive personal data is afforded a higher level of protection. Personal data is anything that can identify and individual e.g. name, NI number, student number, address, date of birth. Sensitive personal data is information about an individual's race, ethnicity, commission of a criminal offence (or the fact they have been subject to criminal proceedings), political opinions, religious beliefs and their membership of a trade union.

EMPLOYEE RESPONSIBILITIES

All staff are responsible for safeguarding personal information and must ensure that personal data is processed for specific and justified purposes. Sometimes this means individuals must give their consent before personal data can be processed.

- You must always be careful and thoughtful when working with information that could be used to identify or be linked to a pupil, parent or member of staff
- You must consider whether you need personal data to achieve your objective
- You must only process the minimum amount of personal data required to perform a task
- You must do everything you can to safeguard the personal data that you access and use. Use common sense, especially when handling sensitive personal data such as pupil premium status and medical conditions. Think carefully about who actually needs to know this information and where you hold any conversations to ensure no one can overhear
- You must only disclose personal data when you have an individual's consent to do so or where there is another legal basis for doing so.
- You must ensure you verify the identity and contact details of a contact before you disclose the personal data
- You must report a suspected data breach to the Principal and DPO within 48 hours

Email

- Personal email addresses must not be used for any work related correspondence
- Wherever possible emailing of personal or sensitive data should be avoided, if it is necessary to share personal data consider if this could be done using Google Drive
- If emailed, any sensitive data must be attached using a password protected and encrypted document, the password must not be included in the original email but should be separately sent or use a password that is already known to the recipients
- Personal data must not be used in the subject of the email, e.g. *John Smith Allegation*
- File names attached to emails must not contain personal data, e.g. *JohnSmithExclusion.doc*
- Double check the recipient list before sending any email containing personal data
- Do not forward email chains without checking the entire content for personal or sensitive information

Commented [A1]: Should this state personal and sensitive data?

IT and Shared Drives, Folders & Files

- The use of USB pen drives and other unencrypted removable media is not permitted in any circumstances
- You must always lock your computer or laptop if left unattended for any period
- Access / Login ID's, usernames and password details for secure systems must be kept secure and not shared
- If personal data is included in any part of a shared network drive folder, such as a staff shared drive, access must only be granted to users who have a legitimate reason to access the information. Access to these shared drives must be controlled by the Network Manager or Senior IT Technician
- If personal data is included in any part of a Google Drive file or folder which is shared, access must only be granted to FCAT domain email addresses. Access to and the content of shared drives are the responsibility of, and must be controlled by, the owner of the file or folder
- If you intend to add a document containing personal and/or sensitive information to a shared location, you are responsible for checking that no unauthorised user will have access to the information once it is shared
- You must check with FCAT's Network Manager or the DPO that any service, app or software you use that requires sharing personal data, such as pupils' names, has appropriate data protection security measures in place and are to safe use
- Before signing up for any external service, app or software that requires sharing of personal data, a Google Form giving details of the service must be completed and submitted for approval by FCAT's Network Manager
- Personal or sensitive data must not be uploaded or shared on social media, online forums or any other online platform
- Any personal IT equipment used e.g. mobile phones, tablets, home laptops, must have access restrictions enabled such as passcode and fingerprint recognition to unlock devices.
- Personal data must not be stored on unencrypted devices e.g. hard drives of personal computers

Other

- When no longer needed, paper documents containing personal data must be shredded or placed in the confidential waste bin
- Paper records that are retained must be kept in a locked filing cabinet and the key locked away
- You must remove confidential information from your workspace and lock this away if you leave for any period of time
- Personal data in electronic or paper form, should only be taken off site when necessary and must not be left in an environment where access cannot be controlled. You must take necessary steps to ensure that the information is kept safe and secure at all times
- Staff or student files which are taken off site and contain personal data, must be signed in and out using an academy personal records register

Commented [A2]: Added a bullet point regarding locally shared network drives. Who has overall access control in each school?