DATA PROTECTION

A Quick Guide for All College Staff

The way in which employees look after and handle other people's personal data is strictly governed by legislation. If you handle any information about identifiable people, like students or staff, then you are dealing with personal data. You need to be especially careful with sensitive information such as health, sexuality or ethnicity.

This Quick Guide is designed to help us all understand what we need to do. Detailed procedures, guidance, training and resources are available from the College's data protection overview page.

PRINCIPLES AND RIGHTS

Personal data must only be used for the purposes it was provided for, as described at the time of collection. It must be relevant, accurate, treated confidentially/securely, and only retained for as long as it is needed (the College's Data Protection Procedure and Code of Practice lists timeframes for the disposal or removal of old records). A good rule of thumb is to consider whether someone would be surprised about how you are using their personal data (check the College's core privacy notices on the website to see what they have been told).

Be aware of people's rights: people have a right to know what happens to their personal data and to see copies of it, including emails. They can ask for inaccuracies to be corrected and they can object to how their personal data is being handled, even asking for it to be deleted. Any formal requests you receive should be passed to the College's Data Protection Officer.

SHARING AND RISKS

If you need to share personal data with another organisation you first need to be sure that all of the risks have been considered. A written agreement in the correct form may be required. If you are unsure about what to do, speak to your line manager or to the College's Data Protection Officer.

If you are starting a new project or initiative involving personal data, make sure you consider data protection issues early on.

POSSIBLE BREACHES

If you think there has been a leak ("breach") of personal data, make sure you report it as soon as possible, including details of the personal data involved and how widely it may have spread. **Use the College's Data Breach Procedure**. The College has to report serious breaches to the Information Commissioner's Office (the regulator) within 72 hours of discovery.

HANDLING PERSONAL DATA IN YOUR WORKSPACE

🔒 If you have leave your office for a short period and personal data is on your desk or shelves, **lock your room** when you leave it.

🔒 Store files and documents about people in **locked drawers and cupboards**. Know where documents are kept and who has access to them.

🔒 Ensure **confidential waste is shredded** or stored securely for collection.

🔒 **Use a strong password**, change it when needed and don't share it with others.

🔒 **Lock your PC screen** when you leave it unattended and log out at the end of the day.

🔒 **Orient your screen** so it can't be viewed by others.

🔒 **Never let others use your computer accounts**.

🔒 **Use passwords/access permissions to protect files** and folders on shared drives storing sensitive data.

🔒 **Beware of unsafe websites**.

HANDLING EMAILS AND PHONE CALLS INVOLVING PERSONAL DATA

🔒 **Don't copy emails about people wider than you need to**.

🔒 **Check email addresses** before you send out personal data.

🔒 Consider sending personal data in a **password-protected attachment** rather than the body of the email.

🔒 If you are sending an email to a group of people, especially if it contains anything sensitive, **think about using "bcc"** so you don't share their addresses.

🔒 **Don't keep emails** about people that you or the College no longer need.

🔒 Be careful when opening emails and attachments from **unknown or suspicious sources**.

🔒 **Don't give out personal data over the phone** about others unless you have verified the caller's identity and you're sure they have a right to have it.

🔒 Generally, don't supply others' contact details or other personal data to unknown enquirers: **take the caller's number** and offer to pass messages/queries on.

🔒 **Pass requests from the police** and other law enforcement agencies to the College's Data Protection Officer.