General Data Protection Regulation (Guidelines for Staff)

Introduction

The General Data Protection Regulation (GDPR) came into effect in May 2018. The core principles of Data Protection remain unchanged. We should:

- Only use personal data when we need to and only use enough to meet our objectives
- Be transparent about how and why we use the data
- Have a lawful basis for using the data
- Allow for inaccurate personal data to be corrected and kept up to date
- Destroy data when we have no more use for it
- Have appropriate security measures to protect it against unauthorised access or loss
- Not transfer it outside the EU except when additional security measures are in place

Sensitive data, specified as race, ethnicity, criminal records, political opinions, religion, trade union membership must be even better protected.

GDPR is stricter than previous legislation about when we can use data, what we should tell people about its use, and how fast and in what manner we must respond in the event of a personal data breach. We must also be able to demonstrate our compliance and higher fines have been introduced in the case of non-compliance.

The College's Data Protection policy is available through the college website or, for staff, in the policies folder. All staff are responsible for the College's compliance with the policy and Heads of Department are responsible for ensuring staff comply with the policy and follow these guidelines.

Data Controllers are the Deputy Principal Finance and Resources, Head of ILT and Data Systems, and the Head of Human Resources. The Data Protection Officer can be contacted at dataprotection@riversidecollege.ac.uk. Any one of these can instigate the Incident Management Procedure

Guidelines

Data Minimalisation

- Do you need personal data to achieve your objective? If not don't use it. Delete it when you have finished with it.
- Only collect what you need

Transparency

- Individuals must know how we use their data, why we use it, how long we keep it, who we share it with and what their rights are. This information can be found in the college Privacy Statement, also on the college website.
- If the data or the reason you use data is not included in the Privacy Policy then you should contact dataprotection@riversidecollege.ac.uk and let us know so we can arrange an update or advise otherwise.

Data Sharing (Internal)

- Personal data should only be shared with other staff who have a genuine need to access it.
- Only share the minimum data to achieve the objective
- Let your line manager know
- Make sure sharing data does not add to the risk of unauthorised access (use encryption to a standard acceptable to the college – and by implication to the DfES - when transferring data electronically)
- Do the individuals whose data is being shared know about it?
- If the data being shared is to be used for a purpose that is different to its normal use consider informing dataprotection@riversidecollege.ac.uk for a second opinion
- Storage of personal or DfES data on portable devices should be limited to the absolute minimum. Where a portable device is used to store personal or DfES data it should be put under the control and configuration of the college and suitably encrypted.

Data Sharing (External)

- Do not share data externally unless you have an individual's consent to do so or there is a legal basis for sharing. Ask dataprotection@riversidecollege.ac.uk if you are not sure. E.g., if the police ask for data pass the responsibility on.
- Make sure sharing data does not add to the risk of unauthorised access (use encryption to a standard acceptable to the college – and by implication to the DfES - when transferring data electronically)
- Be confident about that you know the identity of the requesting person.
- If data is being shared on a regular basis there should be a Data Sharing Agreement in place (Information Sharing Agreement) before data is shared.
- Make sure the Data Protection Officer (dataprotection@riversidecollege.ac.uk) is aware that you are sharing data and request advice.
- Storage of personal data on portable devices should be limited to the absolute minimum. Where a portable device is used to store personal or DfES data it should be put under the control and configuration of the college and suitably encrypted.

Keeping data Up to Date

- Always pass requests for amendment to personal data through to the data controller of that data and dataprotection@riversidecollege.ac.uk
- All staff are responsible for keeping data up to date

Security of Information

- Do not leave information unattended

- Lock your computer screen when you are away from your desk. Do not let people look over your shoulder.
- Lock sensitive paperwork away when not in use.
- Choose secure passwords for all your data access devices. A secure password will be 8+ characters and contain upper and lower case letters, numbers and punctuation. Do not use the same as your last few passwords. Do not leave your device unlocked when you are away from it.
- Never let anyone know your password. Change it if you think anyone else may know it
- Avoid using your own devices to store personal data where possible. If it is necessary use encryption. (Follow the guidance in the paragraph on portable devices in the sections on data sharing).
- Use the college cloud-based system rather than other cloud based systems as an alternative to using your own portable device.
- When sharing documents, staff should classify who the document is intended for (Public, Staff Only etc) in the header of the document. From this, the reader can recognise from the beginning whether they have access to a document that they should not have.
- Contact IT Technical Support for help with Information Security if you have any questions.

Document and Data Retention

- Use the college's Document and Data Retention policy to identify data which should be destroyed/erased.
- Let the dataprotection@riversidecollege.ac.uk know if you have data or documents that are not included in the policy or if you are unsure.
- Heads of Department should make it clear to staff what records are due to be destroyed. Staff should report what records have been destroyed to their line manager and dataprotection@riversidecollege.ac.uk
- Delete your emails when they are more than two academic years out of date. Save important information contained in emails to a more secure location.
- If you have difficulty deleting/ destroying records contact dataprotection@riversidecollege.ac.uk
- Where appropriate mark records with a deletion/destruction date where possible when they are initially filed. It will save time later.

Data Subjects' rights

- Individuals have the right to access their personal data, to request it be deleted, and to request the college stop using it a particular way. (e.g. request we stop sending them marketing emails)
- Any requests must be passed on to one of the college's Data Controllers or dataprotection@riversidecollege.ac.uk as soon as possible so the correct response can be advised. The legal timescale for such a response is currently 40 calendar days.

Personal Data Breaches

- A personal data breach is the destruction, loss, adulteration, unauthorised disclosure of personal data or unauthorised access to personal data. Data can be information in any form including paper records.
- Personal data breaches must always be reported to you line manager and dataprotection@riversidecollege.ac.uk at the first possible opportunity including out of

normal college hours. There is a legal requirement to report serious data breaches to the information Commissioner within 72 hours of the breach being discovered.

- If you know or suspect a personal data breach has occurred you must report it
- You will need to report how the breach occurred, what data and who it affects.
- Loss of a data storage device should be reported in the same way if there is any likelihood of there being a data breach.

Useful Links:

Information Commissioner's Office - Guide to data protection