ID CARDS AND DATA PROTECTION

All employees, students and visitors to the College’s premises must be readily identifiable. This means that security, reception and other staff and students should be able to identify a person on campus, usually by comparing their face to the photograph on their College identity card.

For this reason, while on campus, staff, students and visitors must wear their College Identity Cards or visitors’ cards and these must be visible.

College Security Staff have the right to ask individuals to identify themselves by comparison with their photograph on their ID card. Anyone who refuses permission for them to do so may be removed from the College’s premises.

What information is held?

Information collated from an individual’s Card activity, when it is used to gain access, is collected by the Security Access Control System (SACS). The information that is recorded comprises the date and time at which a badge number has used a reader. The number is related to a person’s name, their photo, CID, department and their access levels. If the user is a student, their end date is also collected. The data is held on a server, managed by ICT.

(NB Where College Identity Cards are used at till points in retail areas on College premises, no personal information is collected. The only information recorded is whether it is a staff card or a student card that is presented, for the purpose of defining the VAT treatment of the purchase with HMRC. It is not possible to collect this information adequately from showing the card as opposed to swiping it.)

Why is this information held?

The information is recorded for the purpose of investigating incidents where knowing who was in the area at a particular time would be of assistance.

How long will this information be held for?

Under the Data Protection Act, the College is only entitled to hold personal data for as long as is necessary for its purpose. In the case of College Identity Card data regarding access, the information will be held for up to 97 days, with a back-up tape held for up to 187 days. The back-up tapes are recycled and the back-up files are overwritten with the new back-up.

The security department feels this to be a reasonable amount of time (taking into account JISC recommendations and best practice) to enable it to carry out an investigation in circumstances when an incident has occurred.

All card holder records are deleted three months after the deactivation date.

Who can access this information?
The data is only accessible by authorised members of the security division and ICT, and will only be accessed in the case of an investigation needing to be carried out. Furthermore, the information is password protected and cannot be accessed without individuals being given access through a firewall. Access to the back-up tapes for the purposes of an investigation can only be authorised by the College Secretary and the Head of Department.

**How can I find out more about the information that is held by the College about me?**

Individuals are entitled to request a copy of information that is recorded about them by making a subject access request under the Data Protection Act. More information about this process can be found at:


**Review of procedures**

The recording and retention of data collected from College Identity Card activity will be regularly monitored in order to ensure that it is achieving its purpose. If procedures are found not to be achieving their purpose then they will be modified.