

## **Case study: Using IT intelligently to reduce risk: Queen Elizabeth's High School, Gainsborough**

One of the risks Queen Elizabeth High School (QEHS), Gainsborough identified early was the potential for any member of staff generating ad-hoc reports in the management information system (MIS) downloading the data onto an unsecure memory stick or personal laptop. It is incredibly useful for staff to be able to download lists of student names, other personal data or exam scores in order to be able to manipulate the data to provide insights into the achievement of groups of students and thereby set the best learning activities for them. However, there was a high risk of data breach if the memory stick or laptop was lost and the data was not encrypted.

Their solution has several layers of security to it in order to control the risks, but without placing an undue administrative burden on the staff of the school. They have provided every member of staff with a memory stick encrypted using a free to use encryption tool. Each memory stick is assigned to a member of staff and logged. No other devices can be used to download files from any computer in the school. Within their GDPR policy and staff behaviour code they have made it clear that no other memory source is to be used and if the data is taken off-site it is not to be loaded onto unencrypted computers at home.

If a member of staff wants a particular data set they email a member of the office staff who has received training indicating what data they want, why they want it and for how long they will keep the data. All of this information is logged so that the school has a record of all data exports that have been undertaken.

The data is then extracted as a spreadsheet, zipped, password protected and placed in a secure area of the school network for a limited time in order for the member of staff to collect it. The password is emailed to the member of staff separately.

As a result, QEHS Gainsborough are confident we have controlled the risks sufficiently to allow staff to continue to use this data as they did before in order to enhance our support for the students whilst protecting the data sufficiently to meet the requirements of the GDPR.