University of East Anglia

SEN17D009

Title:	***Data incident – June 2017***
Author:	Registrar and Secretary Brian Summers
Date:	25th October 2017
Circulation:	Senate 8 November 2017
Agenda:	SEN17A001
Version:	Draft
Status:	Open

Issue
An update on the data incident experienced in June 2017.

Recommendation
Recipients are invited:
To note

i. the summary of the incident published on the University portal
ii. the recommendations made by the independent internal auditors and the University's response and action plan published as part of the above summary
iii. a summary of the outcome of the Information Commissioner's investigation

Resource Implications
The recommendations have resource implications in terms of staff time and systems development.

Risk Implications
The implementation of the recommendations will reduce the overall level of risk facing the University in relation to data security

Equality and Diversity
There are no equality and diversity issues associated with the recommendations.

Timing of decisions
The recommendations have been accepted by the University and the action plan has completion dates attached to each element.

Further Information
For further information please contact the Acting Registrar and Secretary, Ian Callaghan (i.callaghan@uea.ac.uk, x 2208)

Background
The papers were produced to inform staff and students about the data incident itself and the University's response. The incident was also investigated by the Information Commissioner and a summary of their findings has also been made available to staff and students.

Attachments
Appendix 1 - Data incident June 2017 – a summary of the incident, the University's response, the recommendations from the independent internal auditors and the University's action plan

Appendix 2 - Outcome of Information Commissioner's Investigation

Appendix 1

DATA INCIDENT JUNE 2017

An emailing error in June 2017 led to the personal data of a number of students being circulated to a student group email address. The University recognises that the incident is a serious matter and immediately informed the Information Commissioner. The University is continuing to liaise with the Information Commissioner and is responding to her inquiries. Support for the students affected was put in place and continues to be available as we start the new academic year. The independent internal auditors were asked to undertake an investigation and to make recommendations to ensure that steps are taken to minimise the risk of a recurrence and to improve the handling of personal data more generally. The independent internal auditors completed their report in September.

The report itself contains personal data which, along with the terms of the audit contract, restricts the University from publishing the report. The report has been considered by the senior management of the University and we have taken a number of immediate actions to improve the handling of personal data. The report will also be reviewed by the University's governing council. Whilst we are unable to publish the full report we are publishing the following summary of the incident and the recommendations made by the independent internal auditors, and the University's response to them.

The Incident Itself

The Learning and Teaching Service (LTS) undertakes the administrative processes necessary for the student journey from commencement to graduation. There are three administrative "hubs" within LTS that cover different schools. The hub involved was the Arts Hub that supports the School of Art, Media and American Studies (AMA).

LTS operates a shared drive where information relating to the business of LTS is held. The information can be accessed from the shared drive, amended or updated, and securely returned directly to that location by LTS staff.

A member of staff who was updating information concerning extenuating circumstances (personal circumstances which might affect a student's performance in assessment or examinations) had not been provided with access to the shared drive. The information was, as a consequence, provided to the staff member as a spreadsheet attachment (that was not password protected). The information was being collated for consideration by a panel on behalf of the examining board for AMS (a sector of AMA). Following the updating process the spreadsheet was intended to be sent to an internal LTS address that began with "ams…". The autofill function in the outlook email provided a number of options beginning with "ams…" and unfortunately an incorrect address was used, which was a group email address covering some 298 students. The attachment contained personal data relating to 191 students.

The immediate Response to the Incident

The original email was sent at 11.38 on 16 June. The error was reported by students to the front desk of LTS and the Vice-Chancellor's office. By 11.56 attempts had been made to recall the email and requests had been circulated to the group email address asking that it be deleted without reading. By 13.34 IT services had deleted 298 emails from UEA student email accounts of which 172 emails were unread.

In the course of the day, the 298 students on the group list (including the 191 students actually affected) were contacted and warned that their personal data might have been inadvertently disclosed. The University informed the Information Commissioner of the incident.

A small number of students had forwarded the email (and the attachment) to four media outlets. This led to some coverage, particularly online. The media described the incident and some detail of the extenuating circumstances involved, albeit not naming any students. One outlet showed screenshots of the covering email, including the name of the sender.

Starting at 14.35 on that day the University made repeated representations to the media outlets involved that they should take down any details of extenuating circumstances and delete the email attachment from their systems. Eventually assurances were received from all four that they had done so.

The University's response to contain the damage caused by the error was timely and appropriate. However, there were some errors in the email communications (which had to be corrected subsequently) and the original email notifying affected students was distributed more widely than was absolutely necessary.

The visibility given to the name of the sender of the email was regrettable. The University does not consider the sender to have been responsible for the incorrect use of email in this situation, the absence of password protection of the attachment or the selection of the incorrect email address.

Key issues from the independent internal auditors' Report

The independent internal auditors have identified a number of inadequate practices in the University in terms of the structure and use of email systems to communicate personal data (particularly where other, more secure, routes are available) and in the coverage of data protection training.

There were a number of contributory factors leading up to the incident and the absence of any one of them would have avoided the outcome. The shared drive should have been used for sharing the information within LTS, the attachment should have been password protected and the University's email infrastructure could have been configured in a way which, while less convenient, would have reduced the prospect of an incorrect address being selected and, in particular, an address which was a group email.

The use of email to transmit personal information may be more prevalent in LTS (and in the wider University) than is necessary, but where it is essential practices need to be improved and more system-based protections put in place to avoid data being misdirected.

The University's current approach to group email addresses does not clearly signal that an email address is a group address and the makeup of the group. Evidently this was a contributory factor in this incident.

The use of the autofill function increases the risk of an incorrect email address being selected.

All of these issues are being addressed by the University.

Recommendations and the University's Action Plan

The full recommendations from the independent internal auditors are set below, together with the University's response and action plan.

Action plan 1	
Suggested Recommendations – *Methods of sharing information across the University*	**Responsible person / title and target date**
The University should review its processes for sharing information and in particular confidential information through email and identify methods such as password protection and encryption enabling information to be shared effectively and safely. This may include protection of documents containing sensitive data with restriction on printing, forwarding, editing or extracting of data when within emails. Consideration of the use of spreadsheets and similar documents containing confidential information should be made, in particular whether systems should be designed so that reports are only available in an encrypted pdf format ready for use.	
Agreed Action – *Methods of sharing information across the University*	
Following the data incident, the Executive Team tasked a working group (WG) to review and operationalise a number of proposals to limit the risk of a recurrence. The aim is to minimise the use of email as a means of sharing personal data or other confidential information. However, for the short term, and for the longer term where email remains the most appropriate medium, a number of new or enhanced protocols will be put in place. See Action Plans 3 and 5 below. 1. The WG is enhancing policies and procedures around requirements where personal data is sent as an attachment that it is password protected and as part of Data Loss Procedures (DLP) there will be warning messages alerting senders to the attachment and questioning whether it has been protected. The WG expects these measures to be in place by December 2017. It will continue to be a requirement that passwords are not shared via email. 2. The University will implement new DLP tools to provide additional protection in preventing forwarding, editing or extracting data within emails. Software is currently being tested. 3. While Office documents can be encrypted with a password from within the Office application and other restrictions on editing can also be applied (similarly with pdf), the current UEA encryption does not offer protection against misdirection. The WG are currently assessing the options regarding alternative methods of encryption and will make a recommendation in December 2017.	1. & 3. Prof Jacqueline Collier, Pro-Vice-Chancellor and Chair of Working Group (WG) Progressively from now to April 2018 2. Raymond Scott, Assistant Director, Strategy, Policy and Compliance April 2018

Action plan 2	
Suggested Recommendations – *Data Protection Training*	
Data Protection Training should be mandatory for all staff including temporary staff. This should be monitored and uptake reported to management. A culture within the University surrounding Data Protection and sharing of information of 'why' and 'what if' should be adopted and led by management on a continual basis. All temporary staff should be provided with relevant information and training upon arrival into Departments, for example within LTS, the LTS staff handbook.	
Agreed Action –*Data Protection Training*	
1. On 25 July, the Registrar made it mandatory that all academics and support staff should have completed the online Data Protection Training Module no later than 25 September 2017 and that this should then be refreshed on a two yearly cycle. Compliance is being monitored by the Information Compliance Team. Further management/disciplinary action will be taken in any cases of non-compliance. 2. The security of personal data and the risks associated with its sharing and transmission have been discussed at the University's Council, and the Executive and Senior Management Teams in the light of this incident. The content of the current annual reminder to all staff will be reviewed and enhanced as a consequence, and in preparation for General Data Protection Regulation (GDPR). We will introduce (by the end of October 2017) an annual process of cascading direct discussions with colleagues through the organisation to ensure that they actively engage with the issues and develop a predisposition as part of institutional culture, to challenge the need to transmit personal data, and to question whether the necessary protections are in place. 3. All temporary staff are now also required to complete online data protection training and to have read the conditions of computer use as soon as they have an IT account and thus access to UEA systems. This is being monitored by HR for compliance. All managers are being reminded of the need to ensure that temporary staff are inducted in all relevant University and departmental processes and protocols including, in particular, the security of personal data when they will have access to this. *For clarity and to ensure that all necessary action is taken, all actions in this report which are the responsibility of the Registrar and Secretary will pass to the Acting Registrar when the current Registrar and Secretary retires at the end of October 2017.*	Brian Summers, Registrar and Secretary 1. & 3. 25 September 2017 2. 31 October 2017

Action plan 3	
Suggested Recommendations – *Access to group email accounts and IT system access*	
Availability of use of group email addresses should continue to be reduced and redacted for staff where this is not necessary for their particular position within the University. All changes in the nature of employment for all staff at the University should carry a compulsory requirement to review IT access across systems.	
Agreed Action – *Access to group email accounts and IT system access*	
1. Each faculty and division is reviewing all group email lists. Access to group email addresses will be further limited to those staff where their use is a demonstrable and routine requirement of their role. Owners of each group email will be charged with keeping up to date those with authority to access it for sending email. Group email addresses will be moved to a separate section of the global address list. 2. A wider review of the systems for amending user access on changing roles will be undertaken. We see enhancing the technical email security provisions, mandatory data protection training and ongoing awareness raising as providing the main protection against possible email incidents. Overlap of roles (and email permissions) between different types of staff (eg temporary staff and Associate Tutors) will continue to be unavoidable, however we will also undertake action 3 above under Data Protection Training.	1. Prof Jacqueline Collier, Pro-Vice-Chancellor and Chair of Working Group (WG) Progressively from now to April 2018 2. Brian Summers, Registrar & Secretary October 2017

Action plan 4	
Suggested Recommendations – *Access to the LTS Shared Drive*	
Access to Shared Drives and IT access to systems across the University should be reviewed to ascertain if current permissions are relevant. A full review of all data on hard and shared drives should be undertaken across the University on all types of devices to ensure that data is held in-line with Data Protection policies. Use of temporary staff within departments such as LTS undertaking activities with sensitive data should be reviewed by the University.	
Agreed Action – *Access to the LTS Shared Drive*	
The reviews referred to above (current permissions and access to Shared Drives and IT systems across the University and how data on hard and shared drives is held) are being undertaken. They are scheduled on UEA's GDPR roadmap to take until at least May 2018. Initial meetings with all departments will have taken place by the end of 2017. It is inevitable that temporary staff will be involved with personal data from time to time but we will ensure that they are suitably trained to do so (see Action Plan 2 above).	Raymond Scott, Assistant Director, Strategy, Policy and Compliance June 2018

Action plan 5	
Suggested Recommendations – *Email addresses*	
The University should consider amendment to its email infrastructure, including naming conventions of both group and individual emails, for example use of student unique identification numbers and staff and student email addresses being clearly differentiated. We understand the University is looking to suspend the auto-fill email function. The use of the auto-fill email function could be reinstated once email infrastructure within the University is adapted. Consideration of warning messages within the email infrastructure should be made, for example, messages that email is being sent outside of the University or to a large group. Coaching and management of temporary members of staff at the University should be reviewed in-line with the use of temporary staff for handling sensitive data. The incident log maintained by SPC should be extended to detail future decisions regarding reporting to the ICO, based on the guidance provided by the ICO. Review of the University's data incident processes including a gap analysis to the requirements of the GDPR.	
Agreed Action – *Email addresses*	
A new naming convention will be determined and applied to group mailing lists to make it clear that the address is a mailing list, and who will receive emails sent to the list. For instance, if the list is made up of students, the email address should start with 'student'. [The use of student unique identification numbers is not a useful way to differentiate users - and potentially causes its own issues in terms of data protection as the unique number is something we prefer not to publicise.] 2. For September 2017 we plan to modify the display name of personal addresses to indicate whether they are for a student or member of staff (and their department) to also mitigate risk of sending to the incorrect recipient. 3. The options for suspending or modifying auto-fill are being assessed by the WG and will be implemented by December, or earlier where possible.	4. Prof Jacqueline Collier, Pro-Vice-Chancellor and Chair of Working Group (WG) 5. & 6. Raymond Scott, Assistant Director, Strategy, Policy and Compliance) 1. & 2. September 2017 3. & 4. December 2017 5. Complete 6. Dependent on ICO to issue new guidance

4. The University is investigating the options with regard to implementing warning messages which advise that an email will be sent to group email addresses and other recipients such as a shared mailbox and plan to implement he chosen solution by December 2017, or earlier where possible. The implementation of Data Loss Prevention tools (see 1 above) will allow alerts to be raised (and monitored) if a message contains recognisable elements of personal data. 5. SPC recently updated their breach log format and it includes decisions on whether or not the ICO should be informed of personal data breaches, and these are guided by ICO criteria. The breach log already contains a column noting whether the ICO is notified, but does not explain the reasons for that decision – the reasoning is included in the final report/correspondence file. We have now introduced a grading system to assess the severity of all breaches. The outcome of the assessment will be logged. Any assessment above a particular threshold will be reported to the Executive Team for review and further action, particularly where there are lessons to be learnt across the University. 6. Our breach handling process already takes account of the expectations of the GDPR. When the ICO has published further guidance on breach reporting, the process will be reviewed again and updated if necessary.	

Action plan 6	
Suggested Recommendations – *Response plan and execution*	
Complete an in depth review of the University's incident response policy and practices to ensure a co-ordinated response which is accurate, timely and appropriate. This should include consideration of specific review of communications prior to release and support for staff involved. The University should also undertake an exercise to test these plans on a regular basis.	
Agreed Action – *Response plan and execution*	
1. The University's approach to incident response as part of its wider-ranging Business Continuity/Crisis Management procedures is designed to be simple, in order to aid the speed of response. It brings together quickly representatives of all parts of the University that may have a role to play in any particular circumstance, chaired by a member of the Executive Team, to agree the necessary steps for mitigation, remediation and communication. We have reviewed this in the light of the data breach and, as is recognised, this functioned appropriately in terms of mitigation and timeliness. There were communication errors, including giving an impression that a greater number of students might have been affected than was the case and issuing an incorrect email address, which had to be subsequently amended. In fraught circumstances these slips can happen, but we will add to our process a caution that care should be taken in ensuring that only the necessary stakeholders are communicated with and that every attention should be given to the detail of communication. 2. The University will reflect upon the question of support to staff involved in such incidents. Managers will be reminded that the early involvement of HR would be of benefit to ensure that staff are treated appropriately and communicated with effectively. 3. These types of scenarios will be factored into our Business Continuity and Disaster Recovery plans and exercises in the future.	Brian Summers, Registrar and Secretary December 2017

Appendix 2

DATA INCIDENT – JUNE 2017

Outcome of Information Commissioner's Investigation

The Information Commissioner (ICO) has investigated the circumstances surrounding the emailing error which led to sensitive data on a number of students being circulated to a student group email address. After careful consideration the ICO has decided not to take enforcement action on this occasion given the facts of the case and the remedial measures that have already been taken by the University, which the ICO expects to be implemented University-wide, to prevent any recurrence.

The ICO has emphasised the importance of a number of steps that the University is taking to improve compliance with the Data Protection Act and added further detail. The University must ensure that all staff receive data protection and related training on induction, staff should positively acknowledge that they have read and understood appropriate policies and procedures, the uptake of initial and refresher training should be carefully monitored and there should be clarity as to the consequences if the appropriate training is not completed. The University should review policies and processes in the light of this particular incident, and with particular emphasis on the use of internal and external email. Further incidents could result in enforcement action (which can include substantial fines), particularly if the University fails to take steps to reduce the risk of a recurrence.

Notwithstanding the ICO's decision that regulatory or enforcement action is not appropriate to this case, the ICO has made a number of observations concerning the application of the seventh data protection principle, that technical and organisational measures should be taken to avoid the unauthorised processing of (in this case sensitive) personal data. The spreadsheet containing sensitive personal data was circulated within the University without password protection and not all staff involved had received training on the requirements of the Data Protection Act. More generally the levels of completion of data protection training in the University have been poor and there have been other email-related incidents (albeit with lesser impact) where lessons could have been learned related to the risk of using email for transmitting personal data.

The importance of implementing the University's action plan, which will be updated to reflect the detail of the ICO's recommendations, cannot be overstated.