Grantham College & University Centre

CUSTOMER SERVICES POLICY

Data Breach Policy

Computing and Communications Support Services

James Meenaghan

Head of IT Services

June 2022

SUMMARY OF CONTENTS

A	RATIONALE	3
B	POLICY STATEMENT	3
C	ENTITLEMENT	3
D	IMPLEMENTATION	3
	UNACCEPTABLE USE OF COLLEGE COMPUTING SYSTEMS	3
	NON-COMPLIANCE	4
	DISCLAIMER	4
E	EVALUATION	4
	Section 1: Breach of Data	5
	Section 2: Containment and Recovery	5
	Section 3: Assessing the Risk	5
	Section 4: Notification of Data Breaches	6
	Section 5: Evaluation and Response	6
	Section 6: Additional Guidance	6
	DATA BREACH INCIDENT REPORTING FORM	7

Data Breach Policy

A RATIONALE

This document establishes the procedures that Grantham College staff will adhere to in light of a Data Protection Breach. All Grantham College staff have a responsibility to protect College data and ensure that correct procedures are followed if loss of data is reported.

B POLICY STATEMENT

This guidance is intended to supplement the College's Data Protection Policy and has been created in the aim of aiding the understanding of the College's obligations in the event of a data security breach

The College will take the necessary action to ensure that all Computing & Communications systems are protected against unauthorised use.
These include:

- Email and Internet / VLE resources
- Mobile Devices including mobile phones, laptops and tablet devices
- All network resources
- All network user accounts
- Hardware and infrastructure configurations
- All electronic documents

C ENTITLEMENT

This policy and its associated Codes of Practice and Guidelines apply to all users of the College's computing systems. Computing systems users are required to read and comply with this policy and its Codes of Practice as well as any additional guidelines established by the administrators of each system.

BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.

D IMPLEMENTATION

Unacceptable use of College computing systems

For the purpose of this procedure, the following definitions of 'breaches of acceptable use' apply:

- Unauthorised access to system accounts or accounts of other members of the Grantham College community;
- Failure to protect electronic data
- Failure to use encryption if available to protect College data
- Failure to report a loss of College data to the Data Protection Officer
- To assist others in the removal of College data that they are not authorised to have

Non-compliance
Non-compliance with this Policy may pose a threat to the security of the College Network, the privacy of staff, students and other persons and may expose the users of the system or other persons to legal liability. Non-compliance with this Policy is therefore deemed to be a serious matter and appropriate action will be taken when a breach of the policy is identified:

- A failure to abide by this Policy may result in disciplinary action (including revoking or restricting any right to use electronic communications) or cautioning, and may lead to more serious disciplinary action in accordance with College Disciplinary Policies;
- A failure to comply by any staff member will be referred to your line manager and then HR and then dealt with in accordance with processes in relation to misconduct or unsatisfactory performance (as applicable).

Disclaimer

- The College undertakes to provide and operate systems with reasonable care and skill, but accepts no liability for any loss or damage a user may suffer from any failure or malfunction of a system;
- Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to other IT material submitted to or processed on facilities provided or managed by the College or otherwise deposited at or left on its premises.

E EVALUATION

General monitoring of computer systems usage is routinely undertaken and reports compiled. Infringements are logged.

This policy and its associated Codes of Practice and Guidelines will be routinely reviewed 2–yearly and in the light of system or legislative changes.

Linked Documents:
Codes of Practice and Guidelines – Computer Systems
Disciplinary Policies

Section 1. Breach of Data

A personal or sensitive data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the purposes of College business.

The College may be liable for fines that could be imposed by the Information Commissioner's Office amounting to up to 20 million euros or 4% of annual turnover, whichever is the greater.

Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Members of staff at the College, who access, hold or process personal or sensitive data for the purposes of the College business must take appropriate steps to ensure no unauthorised or unlawful processing, accidental loss, destruction of, or damage to personal data occurs.

A data breach can occur for a number of reasons, such as:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking attacks;
- Website defacement;
- Offences where information is obtained by deceiving the end user (Malware Email etc)

Section 2. Containment and Recovery

Data security breaches should be contained and responded to immediately upon discovering the breach. An Impact Assessment should be undertaken to identify measures required to contain or limit potential damage and recover from the incident.

The Data Protection Officer will determine if the breach is still occurring, the IT Services team will investigate and if needed seek help from external contractors to resolve the breach if needed.

The Data Protection Officer will decide if there is anything that can be done to recover the data and limit the damage the breach can cause.

All data breaches, actual and potential, must be reported to the Data Protection Officer

All staff should be aware that any breach of this Data Breach policy might result in the College Displinary Procedure being instigated.

Section 3. Assessing the Risk

Some data security breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role (i.e. a laptop is irreparably damaged, but its files were backed up and can be recovered). Following immediate containment the risks must be assessed which may be associated with the breach, Potential adverse consequences to the individuals, as well as, the College itself and the seriousness of the breach must be considered, further to immediate containment.

The following must be considered upon discovering a data breach:

a) The type of data involved

b) Whether the data is sensitive
c) If data has been lost or stolen, whether encryption protections are in place
d) What has happened to the data, such as the possibility that it may be used to cause harm to the individual(s)
e) The level of detail that would be exposed and how this could affect the individual

Section 4. Notification of Data Breaches

Following the completion of the Data Breach Incident Reporting Form, breaches capable of adversely affecting the individuals should be communicated to those individuals for the purposes of ensuring that specific and clear advice is provided on the steps to be taken to mitigate the risks and if any support could be provided.

It must be evaluated whether the Information Commissioner's Office, other regulatory bodies, and/or other third parties such as the Police or bank/building societies should be notified of the data breach.

Breaches will be reported through the internal reporting structure, to ensure that details of any data breach or risks are reported appropriately

Serious breaches may require for a 'media message' to be communicated to individuals concerned and the public at large, dependant on the seriousness and extent of the breach, which should be considered and implemented where appropriate.

Section 5. Evaluation and Response

It is important that data breaches, actual or potential, are documented and investigated and the response to the breach is evaluated in terms of its effectiveness.

Once the initial incident is resolved, the Data Protection Officer will carry out a review of the cause of the breach. The review should identify the cause of the breach with the help of the CCSS team and other members of College staff.

The review will consider:

- Where and how data is held
- Where the biggest risks lie and identify any further potential weak points within its existing measures
- Are the methods of transmission secure?
- Are the methods of storage secure?
- Identify weak points within the existing security measures
- Offer more training to raise staff awareness of the importance of protecting data

If deemed necessary a report recommending changes to the systems, policies and procedures to be considered by SLT

Section 6. Additional Guidance

Additional guidance may be obtained from a member of the Senior Leadership team

Related Policies:

a) Data Protection Policy
b) Staff Computer Use Policy

Data Breach Incident Reporting Form

Name of person reporting the breach	
Date and Time reported	
Department / Area	
Description of Data Breach Please provide as much detail as possible	
How did the breach occur? Please provide as much detail as possible	
Has a breach of this nature occurred before? Please provide details of the previous incident	
How many individuals does this affect? Please provide as much detail as possible	
Are the individuals staff or students?	
What type of data has been lost/ stolen/ compromised? Example: CVs, student or staff information, financial information, contact details etc	.
Whom has the data been released to? (if known)	
Is the data sensitive? Yes / No If yes, please provide as much detail as possible	
Are you aware of the individuals affect? If so, please provide name and contact details	
What steps could have been taken to avoid a data breach?	
Does the data breach concern electronic data or paper based information?	

Was encryption protection in place at the time of breach? Did BitLocker protect the data for example?	
Has the incident been reported to IT Services team? If your account has been hacked, you must change your password immediately	
Has the incident been reported to the authorities? If so please provide details	
Is there any more information the College should be aware of? Please provide further details if possible	
Brief description of any other action taken at the time of discovery Please provide further details if possible	

For use of the Data Protection Officer or Lead investigation Officer

Notification to ICO	Yes/No – if Yes, notified on: Details
Notification to data subjects	Yes/No – if Yes, notified on: Details
Notification to others (SLT, Corporation etc)	Yes/No – if Yes, notified on: Details

Quality Assurance – Version Control			
Review Period:	Annually	**Review carried out by:**	Head of IT Services
Approved by:	Paul Deane	**Date Approved:**	7.7.22
Equality Impact Assessment Date:	June 22	**Last Review Date:**	June 2022