IT policy breach procedure

Draft Version 0.5

Document Location

http://www.ucc.ie/en/it-policies/pending-approval

Revision History

Date of this revision: 31/12/2012	Date of next revision:

Revision Number	Revision Date	Summary of Changes	Changes marked
0.1	1/10/2012	Original	
0.2	20/10/2012	Redrafted based on updates from IT department	
0.3	14/11/2012	Changes suggested by M Farrell and N Geary in internet security meeting	

Approval

This document requires the following approvals:

Name	Title	Date
ISMT		
IS & ER		
OCLA		

This procedure will be reviewed on a periodic basis.

Table of Contents

1. PURPOSE

The purpose of this document is to clarify for management and IT staff, the procedure for handling a breach of existing IT policies arising out of the inappropriate use of technology on the UCC network. The document should provide guidance on the steps to follow to ensure that breaches in IT policies are handled consistently and have appropriate escalation points where required.

2. DEFINITION

The Digital Estate Working Group (DEWG, dewg@ucc.ie)

The DEWG manage the day-to-day running of the university's websites and social media presence. The group implements policy, define standards and agrees content on a weekly basis. It is comprised of IT, Marketing and Communications, Media and Public Relations, Registrar's Office, (reference the Digital Estate Governance Policy for more information).

The Digital Estate Steering Group

The Digital Estate Steering Group comprises representative content directors and interested parties from across the university. These represent the academic, research, student and administrative functions of the university, The Director of IT Services, the Director of Marketing and Communications, VP of Student Experience, Deputy Corporate Secretary and the Academic Secretary are members of the Digital Estate Steering Group.

Low Severity Incident: is deemed, in the opinion of the DEWG, as the issue itself breaches our acceptable usage, but not in a way that is personally damaging to the university or to others.

High Severity Incident: is deemed, in the opinion of the DEWG, as an incident that may result in the following.

- Incidents that may result in disciplinary action against staff or students
- Incidents that may result in the invocation of the university emergency response plan
- Incidents that may result in a legal action or where there are clear legal implications.
- Incidents that may warrant a communication plan for internal or external stakeholders

3. ROLES AND RESPONSIBLITIES

IT Services

To respond in a timely manner to such notifications/communications and to escalate those matters which cannot be resolved with the user(s) involved to IT Director and relevant management team.

IT Director

To chair the Digital Estate Working Group, to escalate issues where required or to agree the action plans of issues from the Digital Estate Working Group

In circumstances where there is reason to suspect that this AUP is being breached to monitor suspected activity

Digital Estate Working Group

- To assess incidents/policy breaches and to agree the next steps.
- To escalate more serious issues where appropriate.
- To manage any operational risk to the university, from breaches of approved IT policies.

Digital Estate Working Group Steering

To act as an escalation point for serious incidents or breaches of policy, examples of these include

- Incidents that may result in disciplinary action against staff or students.
- Incidents that may result in the invocation of the university emergency response plan.
- Incidents that may result in a legal action or where there are clear legal implications.
- Incidents that may warrant a communication plan for internal or external stakeholders.

Office of Corporate and Legal Affairs **(OCLA)** OCLA will sit on the Steering Group and will offer advice on the legal implications for actions of the Digital Estate Working Group.

Head of Department

Will take appropriate action on disciplinary issues as notified to them by staff or will liaise with other heads of departments on complaints notified to them about other staff members. Will engage HR in the Grievance process when/if required.**HR**

Will manage any issues affecting staff via the university's approved staff grievance procedure. Once an issue is escalated to HR, they will manage any further communications with the staff member involved.

VP of Student Experience

Will manage any issues affecting students via the approved student disciplinary procedure. When an issue is escalated to the VP of Student Experience, he manages any further communications with the individuals involved.

4. SCOPE

The scope of this procedure includes all incidents relating to breaches of approved UCC IT polices as listed on our website http://www.ucc.ie/en/it-policies/policies . This includes

- social media issues
- acceptable use issues, such as on email or websites
- security issues, password loss
- notification of loss of sensitive equipment, hardware
- copyright Infringement issues
- cyber bullying or harassment issues.

5. IT Policy breach handling protocol

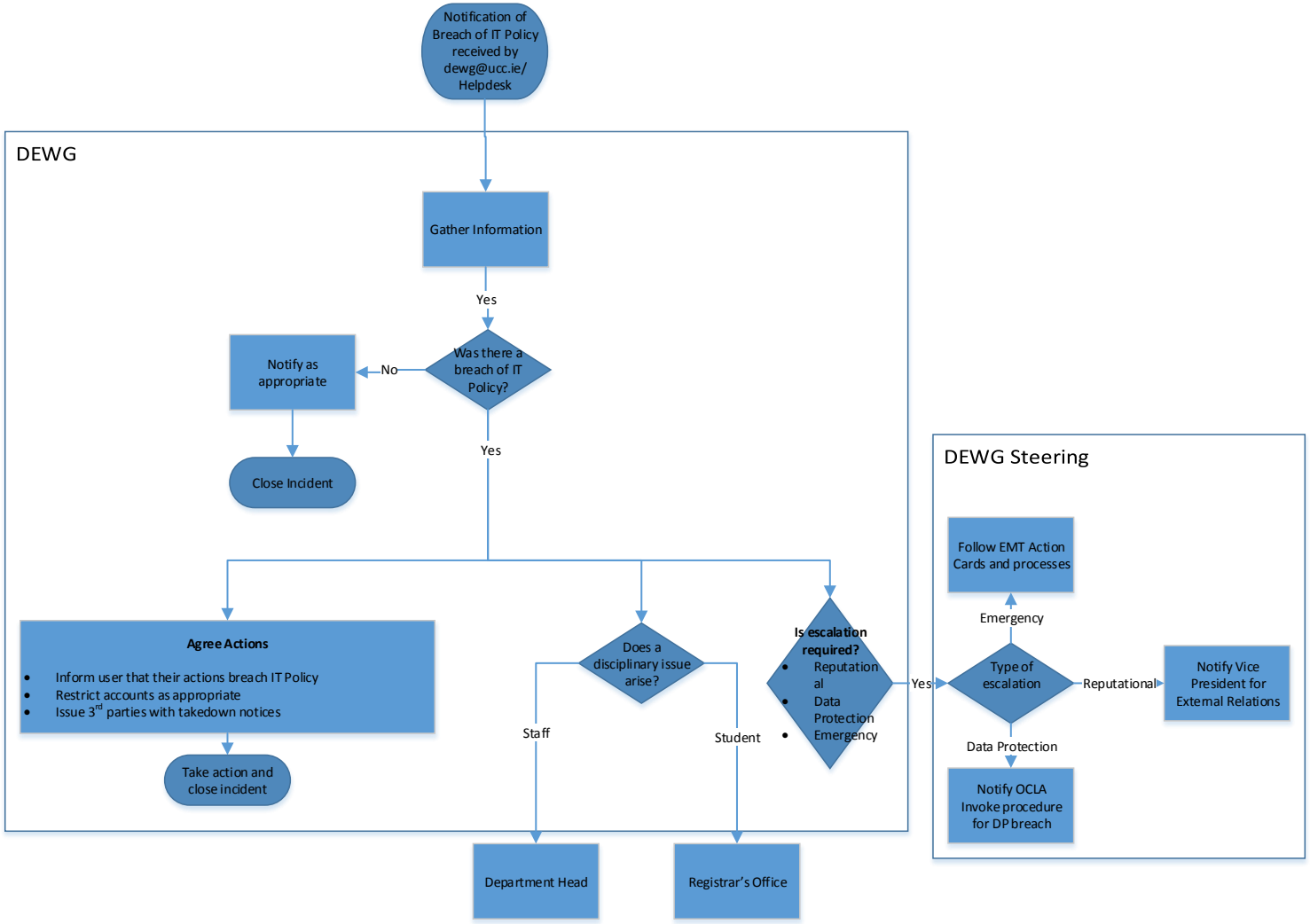

Table 1: Typical DEWG Incident types and actions required

Incident Type	Owner	Action
Copyright breach	OCLA	IT Director will forward to OCLA
Network breach/Hack	IT Director	IT Director will forward to network team
Social Media Abuse	Tom McCarthy	Offensive material will be removed Facebook will be contacted if required
Complaint about Student	Head of Student Experience	Jennifer Murphy will forward to Head of Student Experience
Complaint about Staff	Staff Head of Department	IT will check if the issue is in breach of policy, will offer the staff member their opinion, staff will escalate to HoD, via the standard Grievance procedure
IT detect a breach of Policy	IT Director	Will inform Head of Department or Head of Student experience about the breach

Table 2: Types of Incidents that will be escalated to the Steering group

Incident Type	Owner	Action
Suspected Staff Disciplinary issues	Head of Department	Ask the user to inform their Head of Department of the incident
Suspected Student Disciplinary issues	Head of Student Experience	Student experience will notify Campus watch and follow process
Reputational Damage to the University	VP of external Affairs	
Data protection breach	Data protection officer	Data protection incident procedure will be followed
Emergency Response Issue	UMT Member	Relevant Emergency response plan followed
Serious IT Incident (outage, Hack, Breach)	Director of IT	IT Director will take immediate actions to address the breach.

Step	Action	Executor
1	The IT Services Helpdesk or the DEWG mailbox receives notification of a breach of IT policy	DEWG/Helpdesk
2	Information is gathered relating to the reported breach of IT policy.	DEWG
3	When the DEWG has sufficient information it decides whether, in fact, a breach of IT policy has taken place. If it is decided that a breach of IT policy has not taken place this decision is communicated to the interested parties and the incident is closed.	DEWG
4a	The DEWG agrees appropriate actions to take in response to the breach of IT policy. The first step will usually be to inform the user involved that their actions breach standard IT policy and request immediate cessation/takedown where applicable. Other possible actions include (but are not limited to) restricting or disabling users' accounts and issuing takedown notices to 3rd party sites such as social networking sites.	DEWG
4b	The DEWG considers whether a potential disciplinary issue arises. Such cases involving students are referred to the Registrar's Office (Head of Student Experience) and in the event of staff, the user that reported the incident can make a formal complaint to their head of department in the first instance and then HR, standard UCC grievance procedure applies.	DEWG
4c	The DEWG escalates serious breaches of IT policy to DEWG Steering	DEWG
5	Examples of breaches of IT policy which will be escalated to DEWG Steering include: • Reputational damage to the University. DEWG will notify the office of the Vice President for External Relations • Emergency response issues. The UMT is notified and the relevant emergency response plan is followed. • Data protection issues. The OCLA is notified and the procedure for data protection breach is invoked.	DEWG Steering
6	The DEWG implements its agreed actions and closes the incident.	DEWG

6. Incident handling examples

Scenario
Low impact: Copyright Infringement notice Mistaken breach of policy, unwelcome social media comments
High impact: Abusive email/ offensive social media complaint made against a member of staff