Data Request Policy

Policy owner	Data Protection Officer	**Approval date and body**	October 24th 2017

1. Purpose

University College Dublin provides information technology services to its users in order to perform work for the University in support of its mission. Data is information created, collected, maintained, and utilised by these users while using these services. The University is committed to maintaining users' privacy, and as a data controller the University is required to comply with its obligations under the Data Protection Acts 1988 and 2003.

This policy sets out how the University responds to exceptional requests outside of standard business practices, to authorise a person or party access to "Data" held in any University supported IT service or University owned device, whether it is provided directly by a University unit or is managed by a third party on behalf of the University. Examples of such requests include, but are not limited to the following:

- To provide business related data in the event that an account holder is incapacitated, leaves unexpectedly or is on extended leave and cannot be contacted. This may include access to an account holder's email, storage, University owned device, etc.
- To provide data to the next of kin or executor of an account holder in the case of bereavement or incapacitation.
- Where the University is sanctioned or compelled by legislation in order to detect or prevent a criminal act.

This Data Request Policy is supplemented by, and should be read in conjunction with, the University's Acceptable Usage Policy (AUP).

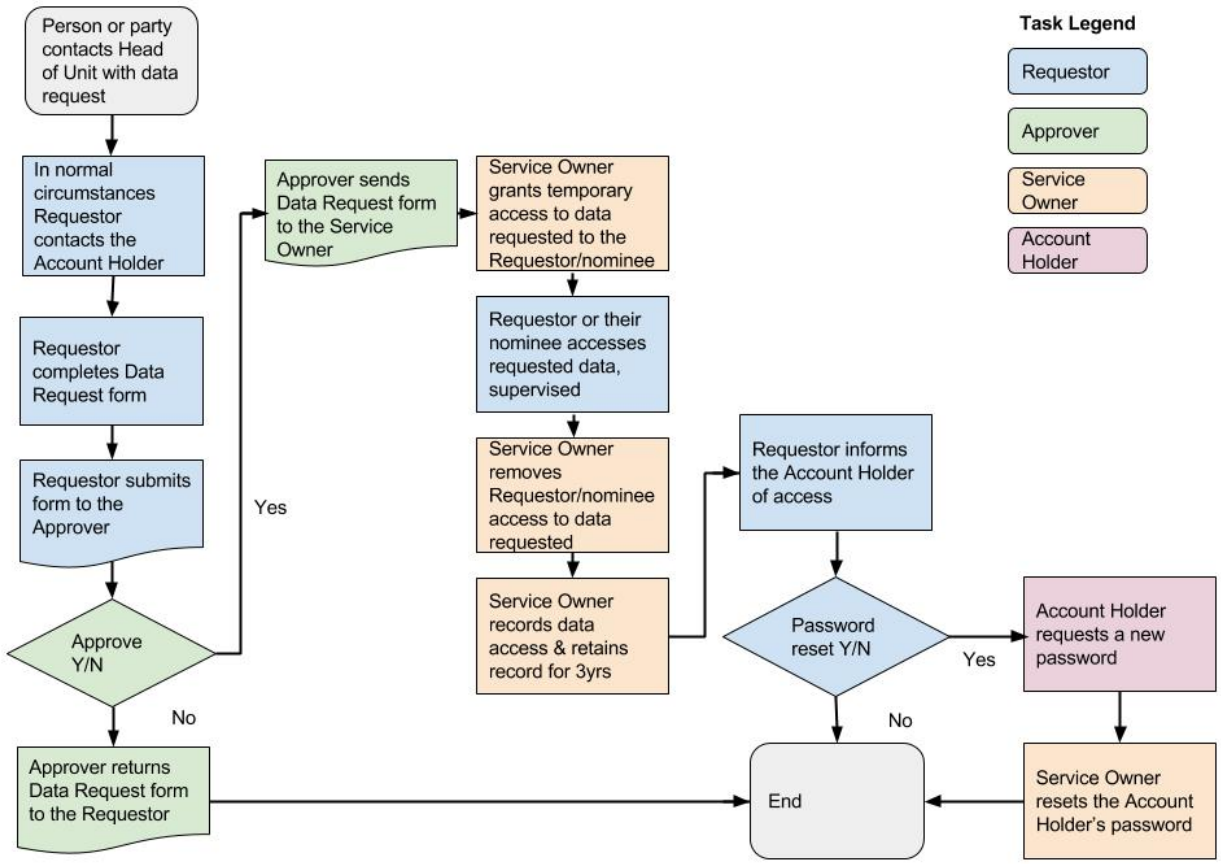
2. Definitions

- The "Account Holder" is an authorised user with data that is stored on a University supported IT service or University owned device.
- The "Approver" is the Data Protection Officer or nominee.
- "Data" is information created, collected, maintained, and utilised by users while using any University IT supported service or University owned device, whether it is provided directly by a University unit or is managed by a third party on behalf of the University. This includes personal data, communications and logs.
- The "Data Access Request Form" is the document that the Requestor must submit in order to be granted approval to access an account holder's data.
- The "Requestor" is the Head of Unit for the Account Holder.
- The "Service Owner" is the unit that is accountable for the IT service regardless of where the technology components reside. For example "IT Services" is the service owner of the University Email service, the University IT network and Novell shared storage.

3. Scope

Exceptional requests to the University, outside of standard business practices, to authorise a person or party access to "Data" held in any University supported IT service or University owned device, whether it is provided directly by a University unit or is managed by a third party on behalf of the University.

4. Procedure



- Person or party initiates request by contacting the Requestor (Head of Unit for the Account Holder) who in normal circumstances will contact the Account Holder to discuss the data access request.

- The Requestor completes the Data Access Request Form and submits it to the Approver. The Requestor must provide the reason why access is required, what data needs to be accessed and what steps will be taken to protect the privacy of the account holder's data, including who will have access and who will supervise access. The *Requestor* cannot be both the *Requestor* and *Approver* for the same request.

- Approved requests will then be sent by the Approver to the appropriate Service Owner to be actioned. For example, in the event that an employee member is absent and can't be contacted and their line manager requires access to their email to retrieve business information the Approver will send the approved request to IT Services to be actioned.

- The Service Owner will then provide the Requestor or their nominee with temporary access to the Account holder's Data for the specified period of time. In the above example, IT Services will provide the Requestor with the Account Holder's username and a temporary password.

- To protect the Account Holder's privacy the Requestor must ensure that the data access is carried out in accordance to the steps outlined in the Data Request form and supervised as indicated on the Data Request form. For Example, in the case of an FOI request for certain email communications a trusted staff member in IT Services will gather the requested data under supervision and will pass the gathered data to the University's Information Compliance Manager who will filter to ensure only the requested data is handed over to the request initiator.

- At the end of the specified period of time, the Service Owner will remove the Requestor or their nominee's access by either resetting the Account Holder's password or by removing privileges granted to the Requestor or nominee.

- After the request is complete, the Requestor is responsible for informing the Account Holder of the reasons why their data was accessed. If the Account Holder's password was reset then they will be required to contact the Service Owner to request a new password.

- Under this policy, each request to access Data must be recorded by the Service Owner and retained for auditing purposes for no less than 3 years.

5. Related Documents

This policy is related to the following existing University policies:

- Acceptable Usage Policy

The policy will conform to UCD's responsibilities under Data Protection legislation.

6. Version History

Name	Version	Date	Reason for issue
Genevieve Dalton	1.0	Jan 2017	UMT Submission
Julian Bostridge	3.6	Jan 2017	Legal review
Genevieve Dalton	3.7	Mar 2017	Change to document name and clarification that the policy is for exceptional data requests only.
Genevieve Dalton	3.8	Jun 2017	Changes following review by University Secretariat.
Genevieve Dalton	3.9	Jun 2017	Changes following review by Registrar and Deputy President.
Genevieve Dalton	4.0	Sep 2017	Editorial changes following review by from Quality Office & EDI review.
Genevieve Dalton	5.0	Oct 2017	Change following feedback from UMT review.
Genevieve Dalton	5.1	Feb 2018	Small change to flow charge to fix error

Data Request Form

A) Details of person making the request (Requestor – Head of Unit for Account Holder)		
Name (in capitals):	**School/Unit:**	
Role:	**Phone ext.**:	
Signature:	**Date**:	
B) Details of Account Holder or equipment to be accessed (Account Holder)		
Name (in capitals):	**UCD Connect username:**	
School/Unit:	**Ext. No.**	
C) **Details of the request:**		
Indicate service or equipment to be accessed: *(UCD E-mail, PC, Laptop, etc.)*		
Indicate person or party who is seeking access to the data:		
Indicate reason why access is required: (Why action is felt to be a proportionate approach)		
Specify exactly what information is required: (Scope of access should limited to only the information required)		
Specify duration access is required: (Specify Dates and times)		
Indicate who will access the data (you or nominee):		
Indicate what steps will be taken to protect the privacy of the account holder and who specifically will supervise the data access:		
Where applicable, indicate how the account holder will be informed their account or data was accessed and the reasons why:		
D) **Approval section (Approver – Data Protection Officer)**		
I approve / do not approve this request to access the data as outlined in section B and C and I am acting in accordance with the Data Request Policy.		
Name (in capitals):		
Role:		
Signature:	**Date**:	
Please send the completed electronic copy of this form (with signatures) to Service Owner. A copy of the completed form must be retained by the Approver for 3 years after approval has been granted.		
E) Access Grant Section (Service Owner)		
I grant / do not grant access the data as outlined in section B and C and that I am acting in accordance with the Data Request Policy.		
Name (in capitals):		
Signature:	**Date**:	