THE UNIVERSITY of EDINBURGH

UNIVERSITY EXECUTIVE
Raeburn Room, Old College
14 May 2018, 10 am

AGENDA

1 Minute — **A**
To *approve* the Minute of the previous meeting held on 9 April 2018.

2 Matters Arising
To *raise* any matters arising.

3 Principal's Communications — **Verbal**
To *receive* an update from the Senior Vice-Principal.

OPERATIONAL ITEMS

4 Widening Participation Implementation & Communication Plan — **B**
To *consider and endorse* the paper by Deputy Secretary, Strategic Planning.

5 Career Track for Staff Specialising in Teaching — **C**
To *consider and endorse* the paper by the Senior Vice-Principal.

6 Planning Round — **D**
To *consider and note* the paper by Deputy Secretary, Strategic Planning.

7 Finance Director's Report — **E**
To *consider and comment* on updates from the Deputy Director of Finance.

8 Complying with extended Research Misconduct reporting requirements — **F**
To *approve* the paper by the Vice-Principal Planning, Resources and Research Policy.

9 Proposal to include Student Residences Requirements in the Network Replacement Project — **G**
To *approve* the proposal by the Chief Information Officer

10 Ethical Fundraising Advisory Group — **H**
To *approve* the paper by the Senior Vice-Principal.

11 Data Protection Policy and Handbook — **I**
To *approve* the policy by the Deputy Secretary Strategic Planning.

12 University Risk Register 2018-19 — **J**
To *consider and comment* on the draft University Risk Register by the Director of Corporate Services

ITEMS FOR NOTING OR FORMAL APPROVAL

13 Fee Strategy Group **K**
To *approve*.

14 Creation of new Chairs and renaming of existing Chairs **L1**
To *approve*. **L2**

15 University Executive Communications **Verbal**
To *note* the key messages to be communicated.

16 Any Other Business **Verbal**
To *consider* any other matters by UE members.

17 Date of next meeting
Monday 11 June 2018 at 10 am in the Raeburn Room, Old College.

THE UNIVERSITY of EDINBURGH

A

UNIVERSITY EXECUTIVE

9 April 2018

[Draft] Minute

Present: Peter Mathieson (Convener)
David Argyle, Chris Cox, Ewen Cameron, Gavin Douglas, Hugh Edmiston, David Gray, Lee Hamill, Gary Jebb, Richard Kenway, Dorothy Miell, Gavin McLachlan, David Robertson, James Saville, Jonathan Seckl, Tracey Slaven, James Smith and Moira Whyte.

In attendance: Fiona Boyd, Kirstie Graham and Judy Robertson (for item 3).

Apologies: Leigh Chalmers, Charlie Jeffery, Andrew Morris, Phil McNaull, Jane Norman, Jeremy Robbins, Sarah Smith and Rob Tomlinson.

1 Minute — Paper A

The Minute of the meeting held on 19 March 2018 was approved.

2 Principal's Communications

The Principal reported that the Director of Finance, Phil McNaull had announced his intention to retire at the end of the calendar year and members of the Executive formally noted their thanks to him; the dispute over the USS pension remained unresolved; the recent series of open forum meetings held with staff and students around the University campuses; a recent visit to Brussels with the Principal of the University of Glasgow, where they had agreed that the two Universities would present a united front on Brexit.

PRESENTATIONS

3 Data Education for All

Judy Robertson, Chair of Digital Learning, gave a stimulating presentation on bringing the benefits of the City Region Deal to local school pupils. The Executive welcomed the ambitious and positive response to the opportunities presented by the City Deal and noted its alignment with the University's strategy on Digital Transformation and Data and Contributing Locally.

4 Digital Disruption and Higher Education

Gavin McLachlan, Chief Information Officer and Librarian to the University gave a presentation on the digital threats to the traditional model of higher education and members noted the issues raised.

STRATEGIC ITEM

5 Developing a University Strategy: Preventing and Responding to Sexual Violence and Misconduct **Paper B**

The University is committed to preventing and responding to sexual violence and misconduct, gender-based hate crime and harassment on its campuses. A "one year on" update of a Universities UK report was published in March 2018 and this provided an evidence base to develop a strategy and programmes of work to respond effectively to this important issue. The Executive considered a paper setting out a number of measures, with the key proposal the establishment of a taskforce with membership from across the University to formulate a strategy and deliver on a work-programme. Members welcomed the University wide approach and noted the important of: encompassing both staff and students, considering broad misconduct issues, including an international dimension and establishing effective relationships with other agencies.

OPERATIONAL ITEMS

6 Planning Round **Paper C**

The Executive noted current progress through the business planning cycle and endorsed EUSA and EUSU's plans, which would be presented to the 23 April Court meeting for consideration and approval.

7 Finance Director's Report **Paper D**

The Deputy Director of Finance spoke to the Quarter 2 forecast which showed an operating surplus to date of £20m, £1m adverse to the profiled forecast to date and £9m favourable to the full year budgeted operating surplus of £11m. This indicated an unrestricted surplus of 2% of gross income, which was the minimum criteria set by Court and was a narrow margin for investment in University operations to meet the aspirations in the planning round. The uncertainty as a result of the USS pension position and potential financial impact was noted, which further underlined the importance of reducing costs and driving up income generation to maintain sustainability.

8 Distance Learning at Scale **Paper E**

The Executive considered a paper setting out the proposed governance model for the first phase of the Distance Learning at Scale Programme, which is a pilot aimed at building, testing and proving the University's and its partners' capability and capacity to deliver distance learning. Whilst content with the governance approach, a detailed business case was required to ensure it was appropriate to continue to scale up distance learning and it was noted that this was being developed.

9 Employee Loan Facility **Paper F**

The Executive approved the proposed employee loan facility via the preferred supplier but requested there was further consideration given to earlier support and financial advice for staff facing financial challenges.

10 Health and Safety Quarter 2 Report **Paper G**

The report was noted.

ITEMS FOR NOTING OR FORMAL APPROVAL

11 University Executive Communications

The key messages arising from the meeting to be communicated more broadly were noted.

12 Dates of Next Meeting

The University Executive will next meet on Monday 14 May 2018 at 10 am in the Raeburn Room, Old College.

THE UNIVERSITY of EDINBURGH

B

UNIVERSITY EXECUTIVE

14 May 2018

Widening Participation Strategy

Description of paper

1. The Widening Participation Strategy 2018-2021, was approved by Court on 23 April 2018. This paper introduces the draft implementation plan and outline communications plan. The draft documents are appended to this paper and, for ease of reference, the approved guiding principles are available on the wiki: Wiki page

Action requested/Recommendation

2. The University Executive is asked to provide feedback on and approve the implementation and communications plans, and to note Court's approval of the final draft of the guiding principles for the Widening Participation strategy.

Paragraphs 3 - 8 have been removed as exempt from release due to FOI.

Risk Management

9. The strategy, and consultation on the strategy, has been designed to minimise risks associated with the under-recruitment of students from disadvantaged and under-represented groups. This should mitigate reputation impacts and compliance threats to SFC funding.

Paragraph 10 has been removed as exempt from release due to FOI.

Equality & Diversity

11. The Widening Participation policy is intended to address the University's responsibilities under clause 3 of the Post 16 Education (Scotland) Act 2013 to address the access to Higher Education of under-represented socio-economic groups.

Next steps & Communication

12. The Widening Participation Strategy Implementation Group will have oversight of the implementation and communication of this strategy, as outlined. This Group will report on progress through the Student Recruitment Strategy Group and the Learning and Teaching Committee.

Consultation

13. The guiding principles for the Widening Participation strategy was approved by Court on 23 April 2018. The Widening Participation Strategy Implementation Group has reviewed and provided feedback on earlier drafts of the implementation and communications plans.

Further information

14. *Authors*
Katrina Castle and Laura Cattell

Presenter
Tracey Slaven

Head(s) of Widening Participation
Student Recruitment and Admissions
Niall Bradley - Deputy Director Marketing,
Gavin Donoghue – Public Affairs Manager,
Philip Graham - Head of Internal Communications
Communications and Marketing
27 April 2018

Deputy Secretary Strategic Planning

Freedom of Information

15. Closed paper - strategy development

THE UNIVERSITY of EDINBURGH

C

UNIVERSITY EXECUTIVE

14 May 2018

Career track for staff specialising in teaching

Description of paper

1. This paper describes our Academic Promotions route and our current offer to staff in roles predominantly focused on teaching.

Action requested/Recommendations

2. The University Executive is asked to discuss the current offer for staff specialising in teaching and to consider whether we should offer additional development routes for Grades 7 – 10.

Paragraphs 3 - 24 have been removed as exempt from release due to FOI.

Risk Management

25. There is a risk that the teaching route is held in less regard than a research route. There will be a potential increase in costs. Consideration will be needed in the development of the new career track to ensure this and the existing routes are 'fit for the future'.

Equality & Diversity

26. A teaching-focused career track may open up career opportunities for staff with particular demographic characteristics. Equality Impact Assessments will be completed should a revised Career track for roles predominantly focused on teaching result in new or revised process.

Paragraph 18 has been removed as exempt from release due to FOI.

Consultation

28. This paper has been produced with input from College HR teams.

29. *Authors*
Karen Lothian
Senior HR Partner – Reward
James Saville
Interim Director of HR
7 May 2018

Presenter
Charlie Jeffery
Senior Vice-Principal

Freedom of Information

30. Closed paper

THE UNIVERSITY of EDINBURGH

D

UNIVERSITY EXECUTIVE

14 May 2018

Planning Round: 2018-21

Description of paper

1. The paper provides an update on the current business planning cycle.

Action requested/Recommendation

2. The University Executive is asked to note progress to date and that a synthesis of the plans and the finalised budget proposals will be considered by Policy and Resources Committee on 4 June 2018 and Court on 18 June 2018.

Paragraphs 3 - 10 have been removed as exempt from release due to FOI.

Risk Management

Paragraph 11 has been removed as exempt from release due to FOI.

12. The University will maintain a positive focus on diversification of income sources and growth to sustain improvements in research and teaching and international reputation. Each College and Support Group has a risk register which flows into the University's risk register; managed by Risk Management Committee. Senior management also has a number of management levers effectively utilised in previous years to control costs when necessary; including tighter controls on recruitment and extending the phasing of capital costs.

Equality & Diversity

13. Equality and diversity is considered within the plans of the individual budget holders

Next steps & Communications

14. The plan and proposals for investment, following further discussion between the Main Budget Holders and the Principal, will progress to Policy and Resources Committee on 4 June and to University Court on 18 June 2018.

Consultation

15. The planning round process includes a round table discussion between the budget holders and reviews of the initial and final draft plans by the thematic Vice-Principals in addition to meetings between the Planning Triumvirate and individual budget-holders.

Further information

16. *Authors*
Jonathan Seckl
Phil McNaull
Tracey Slaven

Presenter
Tracey Slaven,
Deputy Secretary Strategic Planning

Freedom of Information

17. The paper is closed until completion of the business planning round. At that time, the paper will be reviewed before release, for redaction of commercially sensitive material.

THE UNIVERSITY of EDINBURGH

E

UNIVERSITY EXECUTIVE

14 May 2018

Finance Director's Report

Description of paper

1. The paper reports the Period 8, March, University (excluding subsidiaries) Management Accounts and the Quarter 3 University Full Year Forecast for the year.

Action requested/Recommendation

2. The University Executive is asked to comment on the latest update and members can use this report to brief their teams on Finance matters.

Paragraphs 3 - 24 have been removed as exempt from release due to FOI.

Risk Management

25. The University manages its financial risk by not breaching the Group risk appetite as described in its financial metrics; a key one of these is that our unrestricted surplus should be at least 2% of gross income (the Finance Strategy provide a target surplus range of 3% - 5% to remain sustainable). The 2016/17 Financial Reports and the Quarter Three Full Year Forecast demonstrate that we do not expect this indicator to be breached.

26. The continuing health and sustainability of the University depends upon strong direction supported by robust forecasting and we will continue to refine and challenge the assumptions underpinning the Ten Year Forecast.

Equality & Diversity

27. Specific issues of equality and diversity are not relevant to this paper as the content focusses primarily on financial strategy and/or financial project considerations.

Next steps & Communication

28. We would welcome feedback.

Consultation

29. The paper has been reviewed by Phil McNaull, Director of Finance.

Further information

30. *Authors*
Lee Hamill
Deputy Director of Finance
Lorna McLoughlin
Head of FIRST (Financial Information, Reporting & Strategy Team)
1 May 2018

Presenter
Phil McNaull
Finance Director

Freedom of Information

31. This paper should not be included in open business as its disclosure could substantially prejudice the commercial interests of the University.

THE UNIVERSITY of EDINBURGH

F

UNIVERSITY EXECUTIVE

14 May 2018

Complying with extended Research Misconduct reporting requirements

Description of Paper

1. Research Policy Group (RPG) recommends that the University adopts the revised Research Misconduct policy. This will:

- Enable the University fully to comply with the UK Research Integrity Office (UKRIO) Procedure for the Investigation of Misconduct in Research;
- Address UK Research and Innovation (UKRI)'s recent change in Policy and Guidance on Governance of Good Research Conduct,
- Interpret for UoE staff and students the UKRIO procedures.

Action requested/Recommendation

2. The University Executive is asked to approve the attached revised Research Misconduct policy and appendices (list of documents below):

- Revised Research Misconduct policy
- Appendix I Glossary of UKRIO terms and their UoE equivalent
- Appendix II How Research misconduct screening and formal hearing panels would be set up under the UKRIO policy with UoE equivalents
- Appendix III Requirements of UKRI in regard to reporting allegations
- Appendix IV Research Misconduct procedure investigation flow chart with steps from initial allegation to potential disciplinary hearing

Background and context

3. In April 2017, UKRI's predecessor (RCUK) announced a revised *Policy and Guidance on Governance of Good Research Conduct*. Compliance with this is a condition of receipt of UKRI grants.

4. UKRI now expect to be informed at the point at which an allegation of research misconduct is informally investigated rather than only when a formal investigation has begun.

5. In addition, UKRI now reserves the right to have an observer present during formal investigations. The requirement to inform UKRI takes effect once it has been established that allegations are not mistaken, frivolous, vexatious or malicious.

6. UKRI has given limited acknowledgement that universities will need time to revise their procedures to accommodate this change in policy.

Discussion

7. In response, the University Research Ethics and Integrity Review Group set up a working group with representation from Research Support Office, University HR Services (UHRS), Governance and Strategic Planning and the Institute for Academic Development to consider appropriate action. This identified that the University's existing Research Misconduct policy would need to be revised.

8. The working group recommended to RPG that the University used this development to revise the Research Misconduct policy so that the policy and operational procedure also fully complies with the UKRIO's *Procedure for the Investigation of Misconduct in Research*.

9. The decision to direct the reader to UKRIO procedures and to provide them with a glossary of UKRIO terms and roles and their University equivalents rather than develop a new University research misconduct policy brings two benefits.

10. The first benefit is internal. The UKRIO Procedure for the Investigation of Misconduct in Research has been developed so that it is applicable across all disciplines of research. Adopting the UKRIO policy with a translation of UKRIO terms into University equivalences means the University can quickly ensure that it has a research misconduct policy that meets the requirements of UKRI and current/predicted reporting requirements of other research funders such as the Wellcome Trust.

11. The second advantage is external. All the research funders that are signatories to the UUK concordat endorse UKRIO as an independent and expert source of information, advice and guidance on promoting good research practice and investigating allegations of misconduct. On 30 January 2018, UKRIO gave oral evidence to the House of Commons Science and Technology Committee's Research Integrity inquiry. MPs clearly welcomed UKRIO views and the need for greater transparency.

12. In summary, the adoption of a revised Research Misconduct policy that fully complies with the UKRIO Procedure for the Investigation of Misconduct in Research will reinforce the University's commitment to the UUK Concordat on Research Conduct and ensure that the University meets requirements as a recipient of UKRI funds.

Resource implications

13. There will be no additional resources required to communicate and implement the revised procedure.

Risk Management

14. Adopting the revised Research Misconduct policy is intended to ensure that the University at the leading edge in the creation of knowledge and promotes good research practice, as well as having clear and transparent processes for investigating allegations of misconduct. This approach is consistent with the University's threefold appetite for risk in respect of reputation, compliance and finances.

Equality & Diversity

15. It is not expected that the adoption of the revised Research Misconduct policy will disadvantage any staff with protected characteristics.

Next steps & Communication

16. Subject to approval by the University's Combined Joint Consultative and Negotiating Committee on 23 May 2018, the following steps will be taken so that staff

know that the University has adopted a revised research misconduct policy and procedure and understand how to implement the policy, if necessary:

17. *Cross University activity*
    - Email to all staff from the VP Planning, Resources and Research Policy
    - Staff Newsletter to advise staff that the University has adopted a revised Research misconduct policy.
    - Colleges to be provided with boiler plate text for inclusion in College communications
    - The Institute for Academic Development will include the URL to the policy webpage in relevant training material

18. *Cross College activity*
    - The Deans of Research have agreed to take the revised policy to College Research Committees and to ask School Directors of Research to arrange dissemination so that the revised policy is integrated into training sessions for new academic and research staff.
    - Q& A sessions about the practicalities of the adoption of the new policy will be held at College meetings of Research Administrators.

Consultation

19. UHRS developed the revised draft Research Misconduct policy with input from senior College HR and UCU. Information, advice and guidance on best practice from UKRIO Chief Executive has been utilised including detailed feedback on a draft of the policy.

20. Deans of Research and College Heads of HR provided feedback and clarified College implementation arrangements.

21. Members of the Research Ethics and Integrity Group have offered feedback. RPG considered the revised draft policy on 26 February and the trade unions were engaged via HR Policy Development Group, which met on 28 March.

Further information

22. The paper was cleared by Vice-Principal Planning, Resources and Research Policy and the Interim Director of Human Resources.

23. <u>*Authors*</u>
    Dr Susan Cooper (Paper author)
    Governance and Strategic Planning
    Suzanne Mackenzie (Policy author)
    University Human Resource Services
    1 May 2018

    <u>*Presenter*</u>
    Professor Jonathan Seckl,
    Vice- Principal Planning, Resources and Research Policy

Freedom of Information

24. Open paper.

THE UNIVERSITY of EDINBURGH

Research Misconduct Policy

1. Policy Statement

The University conducts research of the highest standard. It is committed to ensuring that all research is carried out with the utmost rigour and integrity. Research misconduct is an uncommon but potentially important threat to rigour and integrity. This policy aims to ensure that any allegation of research misconduct is handled fairly and in line with the UK Research Integrity Office's 'Procedure for the Investigation of Misconduct in Research'.

2. Scope

This policy and procedure will be used to investigate alleged misconduct by current and former employees of the University or by others who conduct research on University premises, or use University facilities, resources or funding for their research.

Allegations relating to the research undertaken by University students will be investigated using the Academic Misconduct Investigation Procedure.

This policy and procedure will also be used to investigate any allegation of research misconduct which is initially raised through the University's Whistleblowing policy[1].

3. Definition of Research Misconduct

Research misconduct includes:

- **fabrication**: making up results or other outputs (e.g. artefacts) and presenting them as if they were real
- **falsification**: manipulating research processes or changing or omitting data without good cause
- **plagiarism**: using other people's material without giving proper credit

[1] Code of Practice on Reporting Malpractice and Raising Concerns under the Public Interest Disclosure Legislation

- **misrepresentation:** for example, misrepresentation of data, of interests, of qualifications or experience, or of involvement, such as inappropriate claims to authorship or attribution of work
- **breach of duty of care:** breach of confidentiality such as disclosing the identity of individuals or groups involved in research without their consent; improper conduct in peer review such as failing to disclose conflicts of interest; or not observing legal and ethical requirements or obligations of care
- **failure to meet ethical, legal and professional obligations**: for example, failure to declare competing interests; misrepresentation of involvement or authorship; misrepresentation of interests; breach of confidentiality; lack of informed consent; misuse of personal data; and abuse of research subjects or materials
- **improper dealing with allegations of misconduct**: failing to address possible infringements such as attempts to cover up misconduct and reprisals against whistleblowers.

The full definition of unacceptable research conduct is available within the RCUK Policy and Guidelines on Governance of Good Research Conduct (Section 3). Allegations of misconduct in research can cover acts of omission as well as acts of commission, i.e. things an individual may have failed to do as well as things they may have done.

4. Principles

4.1 Allegations of research misconduct will be:

- handled with sensitivity and confidentiality
- investigated fairly, thoroughly and in a timely manner
- investigated using the UKRIO Procedure for the Investigation of Misconduct in Research

4.2 Employees have the right to be accompanied to formal meetings by a trade union representative or workplace colleague

4.3 Complainants or respondents have the right to highlight, and have considered, any conflict of interest they perceive to exist on the part of anyone involved in the investigation process

4.4 Employees who make allegations of research misconduct in the reasonable belief that misconduct may have occurred will be supported and will not be subject to any detriment

4.5 Anyone accused of research misconduct is entitled to the presumption of innocence

4.6 The identity of those involved and information on the allegation will not be released to third parties until the University is obliged to do so.

5. Reporting Allegations of Research Misconduct

Anyone who has concerns regarding the rigour and integrity of the research carried out at the University should report these to a Named Person (see Appendix I).

Should concerns be raised by other means, for example through the University's Whistleblowing policy[2], the recipient of these concerns will report these to the appropriate Named Person.

6. Procedure for Investigating Allegations of Research Misconduct

Allegations of research misconduct will be handled in line with the UK Research Integrity Office's 'Procedure for the Investigation of Misconduct in Research'. To support the use of this procedure, a glossary of UKRIO terms and their University equivalent is available at Appendices I and II. A flow chart detailing the procedural steps in University terms can be found in Appendix IV. A high level summary is provided below.

7. Procedure – High Level Summary

- **Initial Steps**: The "Named Person" (see Appendix I) receives the allegation of research misconduct, addresses any immediate risks, informs key senior management of the allegation and informs the person (the Respondent) of the allegation and next steps.
- **Screening Panel**: the Named Person determines if allegations are mistaken, frivolous, vexatious and/or malicious; if this is not the case, the Named Person appoints panel members to determine whether there is evidence of misconduct in research; where contractually required, informs third parties, e.g. research councils, of the allegation

[2] Code of Practice on Reporting Malpractice and Raising Concerns under the Public Interest Disclosure Legislation

without disclosing the respondent's identity. The Screening Panel interviews complainant and respondent and informs Named Person whether there is evidence of misconduct in research and whether they recommend proceeding to Formal Investigation. The Named Person updates all relevant parties of the outcome of the Screening process, including, where contractually required, third parties such as funding bodies.

- **Formal Investigation**: The Named Person, taking advice from their Head of HR, appoints a Panel, made up of at least two senior members of University staff and one external member to investigate the allegation. The allegation is fully investigated, which will include interviews with Complainant, Respondent and other relevant parties. The Named Person updates all relevant parties of the Panel's conclusions, which, for an existing member of staff, could result in a Disciplinary Hearing.
- **Disciplinary Hearing:** If there is a case to answer then a Disciplinary Hearing will be arranged, chaired by a senior manager, usually the Head of School of the Respondent, in line with the University's disciplinary procedure.

8. Cross-Institutional Research

Should an allegation of misconduct involve individuals from institutions other than the University of Edinburgh, the Named Person will contact their counterpart(s) at the other institution(s) to agree:

- whether one institution will be nominated as the lead institution to investigate the allegation, or whether each institution will investigate separately, and
- how each institution will be involved in the process (for example, by providing panel members).

9. Reporting to Third Parties

Where contractually required, third parties such as Research Councils, must be informed of allegations of research misconduct at the start of the Screening Stage of the UKRIO procedure, and updated at all subsequent stages. (See Appendix III for more information on Research Council reporting requirements.) Following investigation, where an allegation of research misconduct has been upheld, the Named Person will inform all relevant third

parties (for example, editors of journals in which the respondent has published articles in order to correct the research record).

10. Policy History and Review

Approval Date:	Year
Approved By:	Committee Name
Year of Next Review:	Year

Appendix I

Glossary of Terms: Roles and Responsibilities

<table>
<tr><th>UKRIO Procedure</th><th>University of Edinburgh Equivalent</th></tr>
<tr><td>Named Person</td><td>CAHSS - Associate Dean (Research Ethics)
CSE - Chair of the CSE Ethics & Integrity Committee
MVM - College Dean of Research</td></tr>
<tr><td colspan="2">The Named Person should be an individual within the organisation with significant knowledge and experience of research and have responsibility for:
a) Receiving any allegations of misconduct in research
b) Initiating and supervising the procedure for investigating allegations of misconduct in research
c) Contacting their counterpart(s) at other institution(s) if the allegation involves individuals from other institutions to agree whether one institution will be nominated as the lead institution to investigate the allegation, or whether each institution will investigate separately. They will also agree how each institution will be involved in the process (for example, providing observers or panel members).
d) Reporting alleged cases of research misconduct to Research Councils at the start of the Screening Stage, and updating them at all subsequent stages
e) Maintaining the information record during the investigation and subsequently reporting on the investigation and outcomes with internal contacts and relevant third parties, as appropriate
f) Taking decisions at key stages of the procedure</td></tr>
<tr><td>Nominated Alternate to Named Person</td><td>CAHSS – Dean of Research
CSE – Deputy Chair of the College Research and Integrity Committee
MVM – Director of Research, Roslin</td></tr>
<tr><td colspan="2">The nominated alternate will receive allegations of misconduct in research and initiate and supervise the procedure for investigating them in the absence of the Named Person.</td></tr>
<tr><td>Head of Organisation</td><td>The Principal</td></tr>
</table>

The Head of Organisation will be informed by the Named Person in confidence when an allegation of research misconduct is received. They will be given:

- the identity of the Respondent
- the identity of the Complainant
- details of all sources of internal and external funding
- details of all internal and external collaborators for the research in question; and
- other details that the Named Person considers appropriate

They will also be informed if the allegation proceeds to a Formal Investigation, and of the outcome.

Head of Research/Head of Finance	**Director of Research Support Office**

The roles of Head of Research and Head of Finance will be informed by the Named Person in confidence when an allegation of research misconduct is received. They will be given:

- the identity of the Respondent;
- the identity of the Complainant;
- details of all sources of internal and external funding;
- details of all internal and external collaborators for the research in question; and
- other details that the Named Person considers appropriate

The Named Person should then, in conjunction with the nominated individuals in Personnel and Finance/ Research Grants Office, investigate the contractual status of the Respondent and the contractual details specific to the research project(s) related to the allegations.

They will also be informed if the allegation proceeds to a Formal Investigation, and of the outcome.

Head of Personnel	**College Head of HR**

The Head of Personnel will be informed by the Named Person in confidence when an allegation of research misconduct is received. They will be given:

- the identity of the Respondent;
- the identity of the Complainant;
- details of all sources of internal and external funding;
- details of all internal and external collaborators for the research in question; and
- other details that the Named Person considers appropriate

The Named Person should then, in conjunction with the nominated individuals in Personnel and Finance/ Research Grants Office, investigate the contractual status of the Respondent and the contractual details specific to the research project(s) related to the allegations. The Head of Personnel will also be informed if the allegation proceeds to a Formal Investigation, and of the outcome. Note: within UoE, the Head of HR will nominate an HR Advisor to attend formal meetings and provide advice on procedural matters. If all or any part of the allegations are upheld, the Named Person, the Head of Personnel and at least one other member of senior staff should then decide whether the matter should be referred to the Organisation's disciplinary process or for other formal actions.	
Representative of Personnel department in attendance at meetings	**HR Advisor**

Appendix II

Membership of Panels

UKRIO Procedure	**University of Edinburgh Equivalent**
Screening Panel - determines whether there is evidence of misconduct in research	
− At least 3 senior members of staff selected by the Named Person from those who have previously indicated their willingness to serve on such a panel. − The panel members will elect a Chair.	At least three senior members of staff selected by the Named Person, one of whom will be asked to chair
In selecting the Panel members, the Named Person should consider: - the subject matter of the allegations, including whether it would be advantageous for members of the Panel to possess any specialised knowledge or investigative skill; - any conflicts of interest that might arise; - any links with any of the persons involved (Respondents or Complainants); - any personal connections with the subject matter of the allegations; and - any connections with the work through, for example, groups established to review proposals for research or ethics committees. It is desirable (especially for cases against senior staff or controversial cases) but not essential that one or more members be selected from outside the Organisation. For joint clinical/honorary contracts, it would be advantageous to have a member of staff from the other employing organisation(s).	
Formal Investigation Panel - considers the allegations of misconduct in research and reaches a conclusion about those allegations. The standard of proof used by the Investigation Panel is that of "on the balance of probabilities". Investigation panels will be set up in line with the UKRIO procedure detailed below.	
− at least 3, and always an uneven number of, senior members of staff selected by the Named Person on the advice of the College Head of HR − panel members must be approved by Head of Organisation (i.e. the Principal) or a nominated deputy (at UoE, this deputy will be the College Head of HR) − one member of the Panel will be appointed as the Chair − at least one member of the panel will be selected from outside the organisation	

<table>
<tr><td colspan="2">

at least 2 panel members will have experience in the area of research in which the alleged misconduct has taken place, although they should not be members of the School/Deanery concerned
where allegations concern highly specialised areas of research, the panel should have one member with specialised knowledge of the field
To ensure a fair investigation, an individual may not be a member of both the Screening Panel and the Investigation Panel, and, if they have been involved in either, they should not be part of the Disciplinary Panel.

</td></tr>
<tr><td colspan="2">Note: Research Councils reserve the right to seek observer status on formal investigations into allegations of research misconduct which involve the councils; this will be by exception, on a case-by-case basis. It is not anticipated that observers would attend full investigations or hearings, but may instead request access to papers and retain the option to be present at key discussions.</td></tr>
<tr><td colspan="2">Disciplinary Hearing</td></tr>
<tr><td>

If all or any part of the allegations are upheld, the Named Person, the Head of Personnel and at least one other member of senior staff should then decide whether the matter should be referred to the Organisation’s disciplinary process or for other formal actions.
To ensure a fair investigation, an individual may not be a member of both the Screening Panel and the Investigation Panel and, if he/she has been involved in either, he/she should not be part of the Disciplinary panel.

</td><td>

The Named Person will advise the College Head of HR of the outcome of the investigation; if the investigation concludes that there is a case to answer, the Head of HR will agree with the relevant Head of School (or College if Head of School participated in the investigation or is the complainant) who will be appointed as the ‘Responsible Manager’ (i.e. who will Chair the Disciplinary Hearing) and the other Hearing Panel members.
Note: panel members cannot be the ‘Named Person’ or anyone involved in the investigation process.

</td></tr>
</table>

Appendix III

Reporting Allegations of Research Misconduct to Research Councils

1. Screening Stage

Research Councils require the University to report research misconduct at the start of the Screening Stage of the UKRIO procedure. The information to be reported by the Named Person is:

- the individual(s)' department
- whether the allegation concerns;
    - research or training directly supported by a Research Council grant or grants and, if so, whether the grant(s) are current or historic
    - research or training that is included in an application to one of the Research Councils, and is still being considered by the Council
    - an applicant on any funding applications currently under consideration by any Research Councils
    - a member of any Research Council advisory panel or body (including any peer review committee or pool)
- the nature of the allegation
- information on any action taken by the University to mitigate or manage risk.

2. Formal Investigation Stage

If, following the Screening Stage, the formal investigation process is triggered, the relevant Research Council(s) must be advised of this by the Named Person.

The respondent's identity should be disclosed in confidence, if:

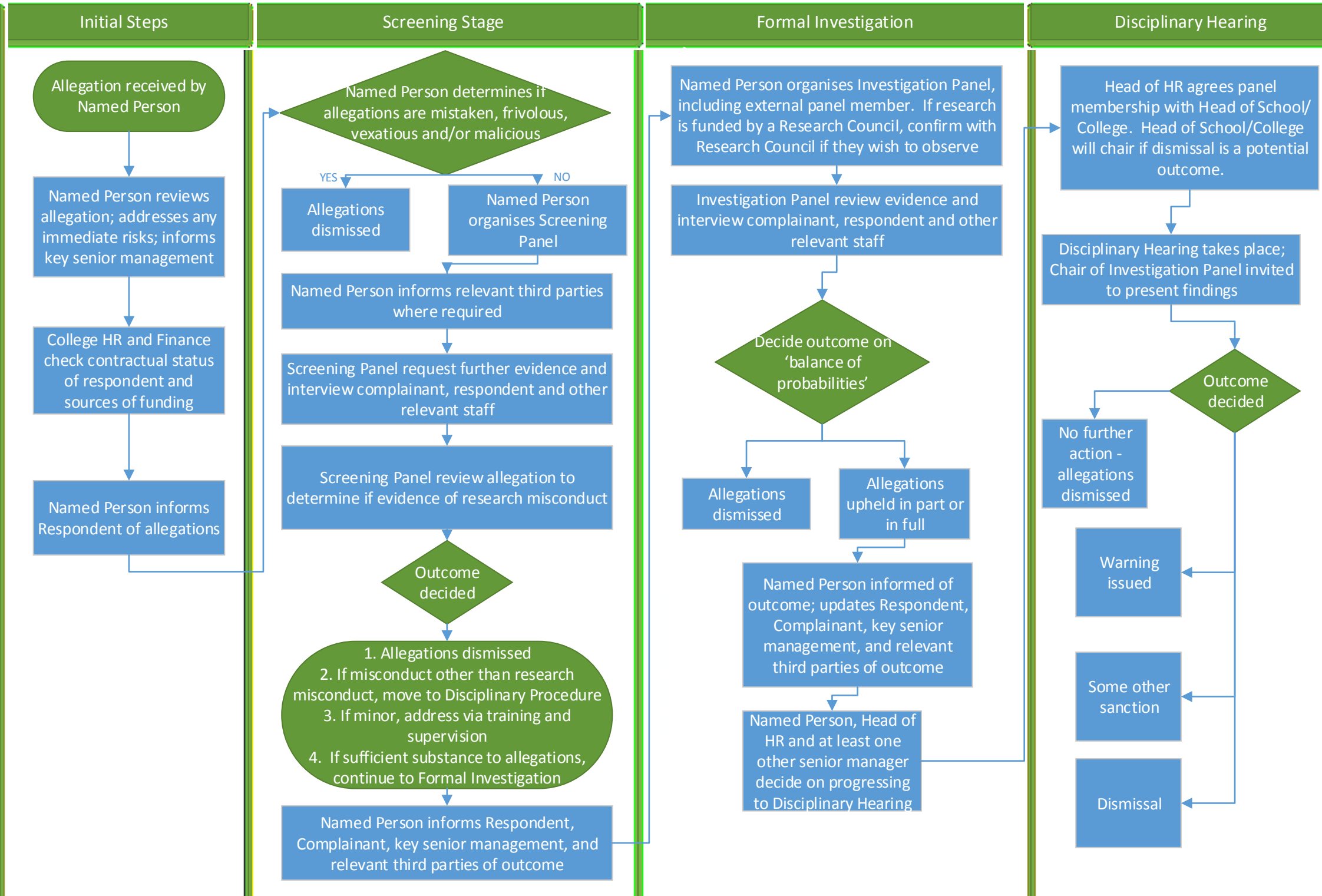
- the respondent is a current grant holder or is being supported by a current grant; and/or
- the allegation concerns research undertaken during a period when the respondent was the Principal Investigator or Co-Investigator of, or otherwise supported by, a research council grant; and/or
- the respondent is currently serving or has served as a member of a research council advisory panel or body at any time since the date of the alleged misconduct.

3. Research Council Action

Research Councils reserve the right to seek observer status on formal investigations into allegations of research misconduct which involve the councils; this will be by exception, on a case-by-case basis. It is not anticipated that observers would attend full investigations, but may instead request access to papers and retain the option to be present.

Research Councils have stated that they prefer not to take any action while investigations are under way. However, they reserve the right do so where the risk of not taking action exceeds the Research Council's acceptable tolerance limits.

Appendix IV: Research Misconduct Procedure



THE UNIVERSITY of EDINBURGH

G

UNIVERSITY EXECUTIVE

14 May 2018

Proposal to include Student Residences Requirements in the Network Replacement Project

Description of paper

1. This paper describes the opportunity to bring the Accommodation, Catering and Events student residences data network and telephony service into the University Campus Network. It also sets out how this could be achieved through the current campus network replacement project.

Action requested/Recommendation

2. The Committee is asked *to approve* the change of scope to the Campus Network Replacement project, which will result in the Accommodation, Catering and Events student data networking and telephony services being provided by Information Services. The Committee is asked to endorse the increased capital to the Campus Network Replacement project.

Paragraphs 3 - 21 have been removed as exempt from release due to FOI.

Equality & Diversity

22. There are no direct equality and diversity implications from inclusion of ACE requirements within the current network replacement project. Equality impact assessments will be performed for any relevant service changes.

Next steps/implications

23. Following support from project board and University Executive, updated requirements would be issued to Bidders through the current procurement process. PRC and Knowledge Strategy Committee will be advised of the change to the requirements and the financial implications thereof and asked to approve.

Consultation

24. Consultation has occurred with Richard Kington, Gavin McLachlan, ACE senior management, ISG Senior management, Estates ISG Strategy group, Procurement, Legal Services, the Network Replacement Programme Board and IT Committee. The Network Replacement programme board endorsed the proposed approach of bringing the ResNet service within scope of the current procurement. IT Committee endorsed the proposed approach of bringing the ResNet service within scope of the current procurement.

Further information

25. *Author*:

Tony Weir
Director of IT Infrastructure
Information Services
Jo Craiglee
Head of Knowledge Management
& IS Planning
26 April 2018

Presenter

Gavin McLachlan
CIO and Librarian to the University

Freedom of Information

26. This paper is closed, due to commercial sensitivity during ongoing procurement.

THE UNIVERSITY of EDINBURGH

H

UNIVERSITY EXECUTIVE

14 May 2018

Ethical Fundraising Advisory Group update

Description of paper

1. The paper provides an update to the membership and terms of reference for the Ethical Fundraising Advisory Group (EFAG).

Action requested/Recommendation

2. The University Executive is asked to approve the revised terms of reference and membership.

Background and context

3. The current principal purpose of EFAG is to consider and advise on whether the sources and purposes of prospective donations, fundraising and other funded activities are ethically acceptable. At the EFAG meeting on 19 March 2018, it was agreed to put forward a number of proposed changes to the Group's membership and terms of reference, as well as undertake a light-touch review of the procedures.

Discussion

4. At the EFAG meeting on 19 March 2018, the following changes were proposed to its membership:

- Professor Peter Mathieson and Dr Anne Richards to stand down as ex officio members of EFAG.
- The Director of Communications & Marketing to join as an ex officio member of EFAG.
- An academic representative from the College of Science & Engineering to join as an ex officio members of EFAG.

5. As a result of these proposals, the following changes are being put forward for approval:

- Professor Charlie Jeffery to be the new Convener of EFAG.
- Alan Johnston, co-opted member of University Court, to replace Dr Anne Richards on EFAG. As outlined in the terms of reference, this change will also be submitted to Nominations Committee and University Court for formal approval.
- Theresa Merrick, incoming Director of Communications & Marketing, to join EFAG.
- Professor David Leach, Dean of Academic Excellence in the College of Science & Engineering, to join EFAG.

6. In addition to the changes of membership, a number of minor amendments to the terms of reference have been made with the aim of tightening the Group's remit. These are all presented in Appendix 1.

Resource implications
7. There are no resource implications in this paper.

Risk Management
8. The procedures for the due diligence review of donations have explicit references to risk. For any donation, members of the University, and in particular staff in D&A, will balance the benefits of funding against reputational risks, taking into account the legal framework and other considerations which will inform the potential decisions of EFAG. The extent of due diligence and of oversight applied will increase in line with an assessment of the risk associated with the potential donor and potential size of the donation.

9. The University Secretary's Group (USG) Risk Register has a risk on "Mishandling of ethical issues (e.g. in fundraising, student recruitment, student services, overseas partnerships, collaborations and consultancy)". Appropriate consideration of ethical issues by EFAG forms part of this risk.

Equality & Diversity
10. Specific issues of equality and diversity are not relevant to this paper.

Next steps & Communication
11. If approved, the new terms of reference and membership will take place with immediate effect. The next meeting of EFAG is on 4 June 2018.

12. As outlined in the terms of reference, an annual EFAG report is to be prepared and presented to the University Executive. The report will also be submitted to the University's Audit & Risk Committee and Risk Management Committee for information. The annual report will therefore be presented at the University Executive meeting on 11 June 2018, along with the light-touch review of the procedures.

Consultation
13. The proposed changes to the terms of reference and membership have been endorsed by EFAG members.

Further information
14.

Author
Jamie Tait
Projects Officer & Policy Advisor
to the University Secretary
EFAG Secretary
May 2018

Presenter
Professor Charlie Jeffery
Senior Vice-Principal

Freedom of Information
15. This paper is open.

Appendix 1 - EFAG Membership and Terms of Reference – June 2018

Membership

Convener: Senior Vice-Principal, Professor Charlie Jeffery ~~Principal & Vice-Chancellor, Professor Peter Mathieson~~
Co-opted member of University ~~Vice-Convener of~~ Court, ~~Dr Anne Richards~~Mr Alan Johnston
~~Senior Vice-Principal, Professor Charlie Jeffery~~
Vice-Principal People & Culture, Professor Jane Norman
Dean of Academic Excellence, College of Science & Engineering, Professor David Leach
University Secretary, Ms Sarah Smith
Director of Finance, Mr Phil McNaull
Director of Social Responsibility and Sustainability, Mr Dave Gorman
Vice-Principal Philanthropy and Advancement, Mr Chris Cox
Director of Communications and Marketing, Ms Theresa Merrick
EUSA Vice President Community, ~~Mr Ollie Glick~~ Ms Georgie Harris

Terms of Reference

1 Purpose

The principal purpose of the Ethical Fundraising Advisory Group (EFAG) is to consider and advise on whether the sources and purposes of prospective donations and philanthropic~~,~~ fundraising ~~and other funded activities~~ are ethically acceptable.

2 Composition

2.1 The Advisory Group shall consist of ~~nine~~ ten members.

2.2 The ~~Principal,~~ Senior Vice-Principal, Vice-Principal People and Culture, Vice-Principal Philanthropy and Advancement, Dean of Academic Excellence, University Secretary, Director of Finance, Director of Communications and Marketing and Director of Social Responsibility and Sustainability shall be *ex officio* members of the Advisory Group.

2.3 The other members of the Advisory Group shall consist of one member of Court and one member nominated by the Edinburgh University Students' Association (EUSA).

2.4 EUSA shall appoint, on an annual basis, a representative to be a member of the Advisory Group. This will normally be the Vice President Community of EUSA who will remain a member of the Advisory Group for the length of their term of office.

2.5 Court shall appoint a member of the Advisory Group on the recommendation of the Nominations Committee.

2.6 The Nominations Committee shall take cognisance of ex officio members of the Advisory Group and ensure that the composition of the Advisory Group is as set out in 2.2.

2.7 The term of office of the Court member will be no longer than their membership of Court unless otherwise determined by Court and shall normally be for a maximum of three years.

2.8 Previous members are eligible for re-appointment up to a normal maximum of two consecutive terms of office.

2.9 The ~~Principal~~ Senior Vice-Principal shall be appointed ex officio Convener of the Advisory Group, and in the absence of the Convener, the University Secretary will act as Convener.

2.10 All members of EFAG are expected to comply with the University's Code of Conduct as set out in the University's Handbook and declare any interests which may conflict with their responsibilities as members of the Advisory Group.

2.11 Other individuals from within or outwith the University may also be invited to attend meetings from time to time, to provide the Advisory Group with information on specific items on the agenda.

3 Meetings

3.1 The Advisory Group will meet as required to fulfil its remit and will meet at least three times each academic year. With the prior approval of the Convener of the Advisory Group, urgent matters may be considered through correspondence.

3.2 Meetings will be timetabled on an annual basis and will take account of the schedule for University Executive meetings to ensure appropriate reporting.

3.3 Minutes, agendas and papers will normally be circulated to members of the Advisory Group at least five days in advance of the meeting. Late papers may be circulated up to two days before the meeting. Only in the case of extreme urgency and with the agreement of the Convener will papers be tabled at meetings of the Advisory Group.

3.4 Non-contentious or urgent matters not on the agenda may be considered at a meeting subject to the agreement of the Convener of the meeting and the majority of members present.

3.5 Papers will indicate the originator(s) and purpose of the paper, the matter(s) which the Advisory Group is being asked to consider, any action(s) required, and confirm the status of the paper in respect of freedom of information legislation.

3.6 Four members of the Advisory Group shall be a quorum. This number must include the ~~Principal~~ Senior Vice-Principal or the University Secretary, who will act as Convener to the Advisory Group should the ~~Principal~~ Senior Vice-Principal be absent for the duration of the meeting.

3.7 A formal minute will be kept of proceedings and submitted for approval at the next meeting of the Advisory Group. The draft minute will be agreed with the Convener of the Advisory Group prior to circulation, and in the case of the absence of the Convener at a meeting, the University Secretary.

3.8 The Advisory Group may also function between meetings through correspondence and any decision(s) taken formally ratified at the next meeting of the Advisory Group.

4 Remit

4.1 To consider and advise on whether the sources and purposes of a) prospective donations (restricted and/or unrestricted) and~~,~~ b) philanthropic fundraising~~, and c) other funded activities~~ are ethically acceptable. Although the University of Edinburgh Development Trust, on behalf of the University of Edinburgh, is grateful to receive support from a wide variety of sources, there are occasions when it might not be appropriate to accept a donation. It is also possible that other matters may need to be referred to the Advisory Group, and it will be the responsibility of the ~~Principal~~ Senior Vice-Principal and University Secretary to agree when matters of this nature require to be considered. ~~This includes funded activities from an individual or organisation that would not ordinarily be considered a donation, which would primarily be raised through Edinburgh Research and Innovation (ERI).~~

4.2 To draft procedures for the due diligence review of donations for approval by the University Executive. The procedures will be reviewed on an annual basis by the Advisory Group, who will subsequently make recommendations to the University Executive if applicable.

4.3 To apply the approved procedures for the due diligence review of donations. As outlined in the procedures, if the Advisory Group is unable to reach agreement or any doubt remains, the matter will be referred to the University Executive.

4.4 To be a sub-group of the University Executive and accountable to it.

4.5 To adhere to the University's commitment to the Principles for Responsible Investment (PRI). Although the remit of the Advisory Group is specifically related to donations, the PRI provides a framework for an organisation to take environmental, social and corporate governance (ESG) considerations into its investment strategies. These principles shall be addressed in relation to prospective donations, fundraising and other funded activities the Advisory Group considers and advises on.

5 Other

5.1 The Advisory Group will from time to time undertake a review of its own performance and effectiveness and thereon report to the University Executive.

5.2 In order to fulfil its remit the Advisory Group may obtain external professional advice as necessary, including seeking legal advice.

5.3 An annual EFAG report will also be prepared and presented to the University Executive. The report will also be submitted to the University's Audit & Risk Committee and Risk Management Committee for information.

5.4 The EFAG terms of reference, membership and procedures will be published on the University's website. Once approved by the University Executive, the EFAG annual report will also be published on the website.

THE UNIVERSITY of EDINBURGH

UNIVERSITY EXECUTIVE COMMITTEE

14 May 2018

Data Protection Policy

Description of paper

1. This paper introduces and seeks approval of a new, General Data Protection Regulation (GDPR) compliant, Data Protection Policy. It is intended to replace the current policy on 25 May 2018, the GDPR implementation date.

Action requested/Recommendation

2. The University Executive is asked to approve the Data Protection Policy and draft Data Protection Handbook (the Handbook), which provides supporting high-level guidance.

Background and context

3. The process of implementing all aspects of GDPR and the new UK Data Protection Act will continue during 2018. This reflects the very short period between clarification of the UK legislation and the date on which GDPR comes into effect and the still evolving advice from the Information Commissioner's Office (ICO).

4. We are using advice from the ICO to prioritise activities. During the Information Commissioner's annual conference on 9 April, the Commissioner advised organisations of her priorities for implementing the GDPR. She pointed out that she expected all outward-facing measures to be in place by the 25 May. This essentially encompasses the Data Protection Policy and preparation and publication of all privacy notices.

Policy and Handbook

5. The Data Protection Policy is a high-level document accompanied by the Handbook. The chapters of the Handbook contain summaries of all guidance that has been produced and links to the full guidance documents. Thus, a single website will facilitate access to all available guidance for staff members. The Handbook will remain in draft format while guidance is still being written.

Privacy notices

6. To improve accessibility to information for both staff and students, two main privacy notices have been prepared. The student privacy notice contains information about the use of student data throughout the time the student spends at the University. New students will receive access at matriculation and existing students will receive a notice via MyEd. The student privacy notice will remain accessible to all students through MyEd during their time at the University.

7. The staff privacy notice contains information about all uses for staff data during employment. New staff members will receive access to the staff privacy notice with their contract of employment and an email with a link to the notice will be sent to all existing staff members.

8. Templates for ad hoc privacy notices for newsletters, mailing lists and events have also been prepared and are currently disseminated on request. A repository for these templates will be created on the GDPR website.

9. For mailing lists and newsletters the privacy notice itself, or a link to the notice, will need to be included in the next communication subscribers receive. If recipients signed up to a mailing list or newsletter, then there is no need to refresh consent. The list owner will only need to obtain consent from recipients if they did not subscribe but were added to the list.

Resources

9. All GDPR implementation projects and processes are integrated into normal planning and are resourced locally. ISG has prioritised implementation within IS APPS workload. We are currently planning additional project management resource to facilitate co-ordination between University-wide and local activities and to provide an Assistant Data Protection Officer (Assistant DPO) post.

Risk Management

10. Compliance with the GDPR will be a statutory requirement. Failure to comply having potentially financial and reputational impacts. The Assistant DPO post will mitigate the risks associated with dependency on a single individual.

Equality & Diversity

11. Enhanced privacy and data protection, objectives of the GDPR, would be expected to support equality and diversity.

Further information

12. *Author*
Rena Gertz
Data Protection Officer
14 September 2017

Presenter
Tracey Slaven
Deputy Secretary, Strategic Planning

Freedom of Information

13. Open paper.

THE UNIVERSITY of EDINBURGH

Data Protection Policy

Introduction

The University of Edinburgh ("the University") is committed to data protection by default and by design and supports the data protection rights of all those with whom it works, including, but not limited to, staff, students, visitors, alumni and research participants.

This policy sets out the accountability and responsibilities of the University, its staff and its students to comply fully with the provisions of the General Data Protection Regulation and the Data Protection Act 2018 (collectively referred to as "the Data Protection Law") and recognises that handling personal data appropriately and in compliance with data protection legislation enhances trust, is the right thing to do and protects the University's relationship with all its stakeholders.

The University holds and processes personal data about individuals such as employees, students, graduates and others, defined as 'data subjects' by the law. Such data must only be processed in accordance with the Data Protection Law.

The University's Data Protection Officer ("the DPO") has responsibility for monitoring and advising on compliance with the Data Protection Law. Responsibility for compliance and the consequences of any breaches cannot legally be transferred to the DPO and is therefore the responsibility of each business area within the University. Information and advice can be obtained from the DPO, from Records Management and from the local Data Protection Champion in every College, School, Department and Support Area.

This policy covers the following areas:

- Purpose of the policy
- Scope of the policy
- Status of the policy
- Responsibilities under the policy
- Data protection by design and default
- Handling of personal data by students
- Data subject rights
- Internal data sharing
- Transfers of personal data outside the EEA
- Direct marketing
- Data protection breaches

A glossary of all definitions used can be found here:
Data Protection Definitions

Purpose of Policy

This policy sets out the responsibilities of the University, its staff and its students to comply fully with the provisions of the Data Protection Law. It is accompanied by a Data Protection Handbook ('the Handbook') with provides information and guidance on different aspects of data protection. This policy and the Handbook form the framework which everybody processing personal data should follow to ensure compliance with data protection legislation. A link to the Handbook can be found here:
Data Protection Handbook (link to be inserted)

Scope

This policy applies to all staff and students in all cases where the University of Edinburgh is the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used.

Status of the Policy

The policy has been approved by the ..... on ….. In common with previous data protection policies, this policy does not form part of the formal contract between the University and staff or students, but compliance with it is a condition of employment and of the Student Contract to abide by the University's rules and policies. Any failure to follow the policy can therefore result in disciplinary proceedings.

Individuals with honorary contracts or 'visitor' status are expected to comply with this policy insofar as they are processing data for and on behalf of the University.
Policy for the Award of Honorary Status.

Responsibilities under the Policy

The University as data controller has a corporate responsibility to implement and comply with data protection legislation. Thus, in determining the purposes for which, and the manner in which personal data is processed, the University must adhere to the six Data Protection Principles ("the Principles") as set out in the legislation. Details of these six principles are found in the accompanying Handbook.

This corporate responsibility is delegated to the Heads of Schools and Colleges and Managers of Administrative and Support Services who have a responsibility to ensure overall compliance with the Data Protection Law and this policy, and to develop and encourage good information handling practices within their areas of responsibility. To meet their obligations, they will delegate the management of but not responsibility for data retention and security to the data stewards. Heads of Schools may choose to delegate the management of, but not the responsibility for, data protection matters within their business unit to the Directors of Professional Services who are supported by the Data Protection Champions. Heads of Administrative and Support Services may allocate responsibility for data protection compliance within their unit to managers who will be supported by the Data Protection Champions. The DPO will perform periodic audits to ensure compliance with this policy and the legislation and will provide regular training to the Data Protection Champions, the Directors of Professional Services and the Data Stewards.

All users of personal data within the University have an individual responsibility to ensure that they process the data in accordance with the Principles and the other conditions set down in the legislation. The Handbook provides detailed guidance to assist with fulfilling these obligations.

Every College, School and Department must nominate one or more Data Protection Champion. These individuals are the first point of contact for data protection questions in their area, escalate difficult questions to the Data Protection Officer and act as a channel of communication between the Data Protection Officer and their area

This section will set out the main requirements for compliance.

Data Protection Training

The University Executive Committee agreed on 12 February 2018 that it should be mandatory for all staff members to complete the Data Protection Training module on Learn. In addition, all academic members of staff must complete the module on "Research under the GDPR". Heads of Schools and Colleges and Managers of Administrative and Support Services are responsible for ensuring compliance. The module can be found here:
Data Protection Training (link to be inserted)

Data Security

All users of personal data within the University must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally. The University's Information Security Policy, the Policy on Taking Sensitive Information and Personal Data outside the Secure Computing Environment and the Computing Regulations must be read in conjunction with this Data Protection Policy.
Information Security Policy
Policy on taking sensitive information and personal data outside the secure computing environment
Computing Regulations

More information can be found in section 4 of the Handbook.

Privacy Notices

When the University collects personal data from individuals, the requirement for 'fairness and transparency' must be adhered to. This means that the University must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data are processed. Any data processing must be consistent or compatible with that purpose. A template and guidance for privacy notices can be found here:
Privacy Notices (link to be inserted).

More information can be found in section 5 of the Handbook.

Conditions of Processing/Lawfulness

In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

a) The data subject has given consent.
b) The processing is required due to a contract.
c) It is necessary due to a legal obligation.
d) It is necessary to protect someone's vital interests (i.e. life or death situation).
e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
f) It is necessary for the legitimate interests of the controller or a third party.

For special categories of personal data, at least one of the following conditions must be met:

a) The data subject has given explicit consent.
b) The processing is necessary for the purposes of employment, social security and social protection law.
c) The processing is necessary to protect someone's vital interests.
d) The processing is carried out by a not-for-profit body.
e) The processing is manifestly made public by the data subject
f) The processing is necessary for legal claims
g) The processing is necessary for reasons of substantial public interest.

h) The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
i) The processing is necessary for public health
j) The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards which are explained in the Handbook

More information can be found in section 6 of the Handbook.

Data Retention

Personal data must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops, mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted. The University's Retention Schedule can be found here and is based on both legal and business requirements:
Retention Schedule

More information can be found in section 7 of the Handbook.

Records of Processing Activities

All Colleges, Schools, Administrative and Support Areas must hold and maintain a record of all processing activities, a so-called Data Processing Register ("the DPRs") to evidence compliance with the Data Protection Law. The DPRs are held centrally by the DPO and will be reviewed on a bi-annually basis.

Data Protection by Design and Default

Under the Data Protection Law, the University has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.

Data Protection Impact Assessment

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an after-thought.
A template and guidance for DPIAs can be found here:
Data Protection Impact Assessments

Anonymisation and Pseudonymisation

Further mechanisms of reducing risks associated with handling personal data are to apply anonymization or pseudonymisation. Wherever possible, personal data must be anonymised or, where that is not possible, pseudonymised.

Guidance on how and when to anonymise and pseudonymise can be found here:

Anonymisation and Pseudonymisation (link to be inserted)

More information on privacy by design and default can be found in section 15 of the Handbook.

Handling Research Data

Before commencing any research which will involve obtaining or using personal data and special categories of personal data, the researcher must give proper consideration to this policy and the guidance contained in the Handbook and how these will be properly complied with. The researcher must ensure that the fairness, transparency and lawfulness principle is complied with and that privacy by design and default is applied. This means that wherever feasible, research data must be anonymised or pseudonymised at the earliest possible time.

More information can be found in section 12 of the Handbook.

Handling of Research Data by Students

The use of personal data by students is governed by the following:

- Where a student collects and processes personal data in order to pursue a course of study with the University, and this course of study is not part of a University-led project, the student rather than the University is the data controller for the personal data used in the research. If the data are extracted from a database already held by the University, the University remains the data controller for the database, but the student will be the data controller for the extracted data.
- Once a thesis containing personal data is submitted for assessment, the University becomes data controller for that personal data.
- Where a research student processes personal data whilst working on a project led by a University research group, the University is the data controller.

Academic and academic-related staff must ensure that students they supervise are aware of the following:

- A student should only use personal data for a University-related purpose with the knowledge and express consent of an appropriate member of academic staff (normally, for a postgraduate, this would be the supervisor, and for an undergraduate the person responsible for teaching the relevant class/course).
- The use of University-related personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be anonymised so that students are not able to identify the subject.

More information can be found in section 13 of the Handbook.

Data Subject Rights

The data protection legislation contains eight data subject rights the University must comply with – the rights to information (see Privacy Notices), subject access, to rectification, to object, to erasure, to portability, to restrict processing and in relation to automated decision-making and profiling. These rights can be restricted for personal data used in research.

<u>Subject Access Requests and the right to data portability</u>

Individuals have the right to request to see or receive copies of any information the University holds about them, and in certain circumstances to have that data provided in a structured,

commonly used and machine readable format so it can be forwarded to another data controller. The University must respond to these requests within four weeks. It is a personal criminal offence to delete relevant personal data after a subject access request has been received.

Individuals receiving a subject access request must follow the subject access request procedures contained in section 11 the Handbook.

Right to erasure, to restrict processing, to rectification and to object

In certain circumstances data subjects have the right to have their data erased. This only applies

- where the data is no longer required for the purpose for which it was originally collected, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require the University to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

Individuals receiving any of these requests should not act or respond but instead should contact the DPO immediately.

Rights in relation to automated decision making and profiling

In the case of automated decision making and profiling that may have significant effects on data subjects, they have the right to either have the decision reviewed by a human being or to not be subject to this type of decision making at all. These requests must be forwarded to the DPO immediately.

More information can be found in section 11 of the Handbook.

Data Sharing

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the students.

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between the University and the third party must be signed, unless disclosure is required by law, such as certain requests from the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes.

More information can be found in section 8 of the Handbook.

Transfers of Personal Data Outside the EEA

Personal data can only be transferred out of the European Economic Area when there are safeguards in place to ensure an adequate level of protection for the data. For transfers of personal data to a receiving party in the United States of America, the Privacy Shield Agreement between the European Union and the United States of America provides sufficient protection. Before transferring data, the Privacy Shield website should be consulted to determine whether the receiving party is on the Privacy Shield List. Staff involved in transferring personal data to other countries must ensure that an appropriate safeguard is in place before agreeing to any such transfer.

More information can be found in section 10 of the Handbook.

Direct Marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For the University, this will include notifications about events, fundraising, selling goods or services. Marketing covers all forms of communications, such as contact by post, fax, telephone and electronic messages, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003. The University must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

More information can be found in section 16 of the Handbook.

Data Protection Training

The University Executive Committee agreed on 12 February 2018 that it should be mandatory for all staff members to complete the Data Protection Training module on Learn. In addition, all academic members of staff must complete the module on Research under the GDPR. The module can be found here:
Data Protection Training (link to be inserted)

Data Protection Breaches

The University is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The University makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of the University's Data Protection Officer who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, the University is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after

becoming aware of it. Any member of the University community who encounters something they believe may be a data protection incident must report it immediately to the IS Helpline at 651 5151 or IS.Helpdesk@ed.ac.uk.

Details of how to report a breach and the information that will be required are included in section 17 of the Handbook.

University Contacts

The University's named Data Protection Officer details are published at:
https://www.ed.ac.uk/profile/data-protection-officer.

Enquiries regarding subject access requests must be addressed to:
recordsmanagement@ed.ac.uk.

Data Protection Handbook

Contents

1 – Introduction

The General Data Protection Regulation and the Data Protection Act 2018 cover all personal data processed by the University, irrespective of where the data is held and what format it is held in.

2 – Glossary

The following terms are used within the Data Protection Handbook and the guidance documents:

The GDPR – General Data Protection Regulation

The DPA – Data Protection Act 2018

Personal Data – Current data protection legislation applies only to personal data about a living, identifiable individual.

Special Categories of Personal Data – Personal data is classed as belonging to "special categories" under current data protection legislation if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life or sexual orientation
- commission of offences or alleged offences
- genetic data
- biometric data

Data Subject – A data subject is an individual who is the subject of personal data.

Processing – Data processing is any action taken with personal data. This includes the collection, use, disclosure, destruction and holding of data.

Data Controller – A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage and deletion of the data.

Data Processor – A data processor is an organisation that processes personal data on behalf of another organisation.

Automated Decision-Making – Automated decision-making takes place where decisions are made solely by automated means without any human involvement.

Profiling – Profiling means automated processing of personal data to evaluate certain things about a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour or movements.

The detailed definitions can be found here:

Definitions

3 – Key considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do you really need to use the information?
- Could anonymised or pseudonymised data be used?
- Do you have a valid justification for processing the data i.e. it is required for a contract or has the data subject given their consent? (see section 6)
- Has the data subject been told about the processing i.e. been issued with a privacy notice? (see section 5)
- Are you sure that the personal data will be secure during the process? (see section 4)
- Are you planning to pass personal data on to a third party or transfer the data outside the EEA? If so do you have the necessary safeguards/permissions in place to do this?
- If you are setting up new systems/processes have the Data Protection by Design and Data Protection Impact Assessment guidelines been followed?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

If having considered the points above you conclude that the processing of personal data is necessary, then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of GDPR and the DPA.

4 – Data Security

The CISO Division, led by the University Chief Information Security Officer (CISO), is responsible for leading and owning the University information security risk strategy. They encourage a risk based approach to provide holistic responses to information security risks. The Division leads pan-University information security initiatives, provides strategic advice on existing and emerging information security threats and delivers security awareness training to support this.

On the Information Security website, you will find all necessary guidance, policies and procedures to ensure that you protect the information you process appropriately. You will also find mandatory InfoSec training you must complete.

Detailed guidance on data security can be found here:

Information Security

5 – Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, the University is required to provide data subjects with a privacy notice to let them know what we are doing with their personal data.

A privacy notice must be:

- easily accessible,
- provided at the time of collecting the data,
- written in a clear and concise way

The University uses a layered approach to privacy notices: The first half which requires to be customised (purpose, legal basis, recipients, retention times, automated decision-making) will be provided directly to the data subject with a link to the second, generic half (contact details, rights, transfers outside the EU), which is located on the University's website and can be accessed from the first half via a link.

The University has two main privacy notices, one for staff and one for students. These notices which will be provided at matriculation (for students) and at signing of the employment contract (for staff) can be found here:

Staff privacy notice (link to be inserted)

Job applicant privacy notice (link to be inserted)

Student privacy notice (link to be inserted)

Student application privacy notice (link to be inserted)

Where personal data is collected outwith these two situations, a separate privacy notice will be provided by the College/School/Department collecting the data. Examples are conference registration and newsletters. Templates for these notices can be found here:

Privacy notices (link to be inserted)

A template for a generic privacy notice and guidance on how to complete the template is provided here:

Privacy Notice Template

6 – Lawfulness

Whenever the University processes personal data in any way, there must be a valid justification, a so-called legal basis for doing so. The GDPR and the DPA provide a list of six legal bases for personal data. If special categories of personal data are processed, the law provides an additional list of legal bases. Thus, for special categories, one legal basis from each of the two lists must be met.

The legal bases to choose from for personal data are:

- consent
- necessary for performance of a contract
- legal obligation
- vital interest
- necessary for the performance of public tasks/core functions
- necessary for a legitimate interest.

For special categories of personal data, the relevant legal bases for the University are:

- explicit consent
- necessary for purposes of employment or social security law
- necessary for reasons of substantial public interest
- necessary for medical purposes
- necessary for archiving purposes or statistics and research.

A full description of these legal bases together with examples for their use can be found here:

Guidance on Legal Basis for Processing

7 – Retention

The GDPR sets a clear requirement for the University to take its data retention responsibilities seriously. Generally, personal data should only be retained for as long as necessary. Just how long 'necessary' is, however, can differ based on the type of data processed, the purpose of processing or other factors. Not only do you have to inform data subjects in the privacy notice how long you keep their personal data for, you will then have to ensure that these retention times are adhered to. This means that data will need to be deleted, destroyed or fully anonymised at the end of the retention time or archived appropriately in the University Archives.

It is important to note that on the other hand, in some circumstances personal data must be kept as destroying such data would be a data protection breach, for example student records to verify a student's qualifications.

Data retention is a personal responsibility for everybody in the University and it is important that you have an overview of where personal data is stored. This may include:

- own servers
- third party servers
- email accounts
- Sharepoint sites

- Shared drives
- backup storage
- paper files

University records should always be stored in a departmental filing scheme, rather than by individuals. For example, you should not run reports and save them in spreadsheets in a folder on your desktop. Systems must be set up to make this less likely to happen in the first place. Staff should use managed desktops or connect remotely where practical.

Detailed guidance on data security can be found here:
Records Management

8 – Data Sharing

You may be asked to share personal data both within the University (by colleagues in your own area or in another unrelated area) and outwith the University (by another organisation). Note that if you use an external company or organisation to process personal data on your behalf (a 'data processor'), the requirements for data sharing do not apply.

Internal data sharing

Internal data sharing, whether with a colleague from your own area or somebody from another unrelated area will usually be unproblematic and is likely to continue. The questions you need to ask are:

- Would data subjects reasonably expect their data to be shared with you and is the purpose for sharing the data consistent with what the data subjects have been told in the privacy notice and do the legal basis and retention periods still apply? Would data subjects reasonably expect their data to be shared with you? The key privacy notices can be found here:
    - Staff privacy notice (link to be inserted) which provides links to other student related privacy notices (such as special circumstances, applications)
    - Student privacy notice (link to be inserted)
- Are there any risks involved in sharing the personal data? If there could be, a Data Protection Impact Assessment should be carried out. (see section 15)

If you have answered these general questions satisfactorily, then the data can be shared. More detailed guidance can be found here:

Internal sharing of data

External data sharing

If another organisation requests that you share personal data, then you will need to ask these questions:

- Does the sharing involve the transfer of data outside the EU? (see section 10)
- Is the third party acting as a processor for the University i.e. acting under the instruction and on behalf of the University?

- Is the third party requesting the personal data for their own use and purpose? Then the third party is another data controller.

If you are setting up a relationship with an outside organisation that will involve the transfer of personal information, you must put in place a contract to ensure that adequate protection is given to that information so that the University meets its data protection obligations and protects the rights of the individuals involved.

There are specific contract requirements depending on the circumstances. For example, the standard terms and conditions of most cloud service providers are not normally sufficient. The University's Legal Services Team and/or IS can provide template agreements to meet the needs of different transfer arrangements. They can be contacted at:
legalservices@ed.ac.uk
informationsecurity@ed.ac.uk

9 – Third Party Requests

The University often receives requests for the personal information of its students and staff from third parties. Detailed guidance on sharing personal data with third parties can be found here:

Sharing Personal Data

Requests from parents, friends or relatives of a student

No release without the student's consent.

It is acceptable to advise the requesters that we will accept a message and, if having checked our records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether or not they are at the University.

More guidance can be found here:

Parents and Family Members

Requests from organisations providing financial support

The University routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in our privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in our privacy notices (e.g private funders) without evidence of student consent.

Requests from Home Office/UK Visas and Immigration (UKVI)

The University often receives requests for information on attendance and other details relating to international students. Information should only be disclosed where we are satisfied there is a legal requirement to provide the requested information or the individual concerned has given their consent. Requests for student information should be passed on to the Immigration Compliance Team at Kate.Monroe@ed.ac.uk.

Requests from the Police or law enforcement officials

The University is not legally obliged to provide information to the police, unless presented with a court order. However, the University will usually choose to release information where the police, or other law enforcement agencies, can demonstrate to

our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders.

For such requests, the established procedure can be found here:

Police enquiries, and similar agencies

Disclosures required by law

There are circumstances where the University is legally obliged to disclose information about an individual to a third party if this is required by law, enactment or court order:

Third Party	*Authorisation for disclosure*
UK Funding Councils e.g. HEFCE HEFCW, SFC and their agents e.g. QAA, HESA, HEFCE auditors	Further and Higher Education Act, 1992 s.79
Electoral registration officers	Representation of the People Act 2000; The Representation of the People (Scotland) & (England and Wales) Regulations 2001
Officers of the Department of Works and Pensions, and Local Authorities	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995 s.3
Audit Commission and related auditing bodies	Audit Commission Act 1998 s.6
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Environment Agency	Agency Regulations – specific ones to be quoted
Inland Revenue	Taxes Management Act 1970
Other third parties	With a Court Order

With such requests, we must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

10 – Data Transfer Outside the EEA

International data transfer can be:

- Sending personal data from the University to an organisation, company or an individual that is based in a non-EEA country.
- Remotely accessing a University database from your computer if at that time you are in a non-EEA country.

These transfers are not prohibited, however, we must ensure that so-called safeguards are in place. The GDPR provides a list of these safeguards, one of which must apply:

- Adequacy of the country: The EU has assessed the third country to have an adequate level of protection. These countries are then treated as though they were an EU member state and data can be transferred there without the need for any further safeguards. The countries that currently fall into this category are:
    - Andorra
    - Argentina
    - Australia
    - Canada
    - Faeroe Islands
    - Guernsey
    - State of Israel
    - Isle of Man
    - Jersey
    - New Zealand
    - Switzerland
    - Uruguay
- Transfers to the USA: For data transfers to the USA, the company or organisation receiving the data has signed up to the Privacy Shield. A list of these can be found here:

  Privacy Shield List
- Contract clauses: If you have a contract with the organisation you are sending the data to, it must include specific data protection contract clauses. Information and templates of these clauses for insertion into the contract can be obtained from Legal Services at:

  legalservices@ed.ac.uk.
- Court orders: You have received a court order requiring the transfer.
- Consent: The data subject has given explicit consent to the transfer, having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards.
- Contract with the data subject: The transfer is necessary for a contract between the data subject and the University, for example when non-EEA students ask for their exam results to be sent to their funding organisation in their home country.
- Contract in the interest of the data subject: The transfer is necessary when there is a contract in place between the University and another organisation, and that contract is in the interests of the data subject, for example when students wish to spend a term abroad. There will be a contract between the University of Edinburgh and the host university and that contract is in the interest of the students.
- Public interest: The transfer is necessary for important reasons of public interest. Examples for this are crime prevention and detection, or national security.
- Lawsuits: The transfer is required for a lawsuit.
- Medical emergencies: The transfer is necessary for a medical emergency.
- Legitimate interest: The transfer is in the legitimate interest of the data controller. This safeguard is only available if the data of only a small number of

data subjects is transferred abroad, if the transfer is a one-off, if the data transfer is secure and if both the Information Commissioner and the data subjects have been informed.

Staff authorising transfers of personal data outside the EU are responsible for ensuring that one of the above requirements is met and ensuring that a record is kept of which safeguard is in place. Where transfers are done on the basis of consent, evidence of the consent and when it was obtained should be kept.

For more advice on transfers of personal data outside the EU please contact the Data Protection Officer or Legal Services at:

dpo@ed.ac.uk
legalservices@ed.ac.uk.

11 – Data Subject Rights

The GDPR lists eight data subject rights that the University will need to comply with, these are the rights of the data subject to:

- Be informed
- Subject access
- Erasure (to be forgotten)
- Rectification
- Portability
- Object
- Restrict processing
- Object to automated processing and profiling

Right to be informed

The right to be informed is complied with by issuing a privacy notice, please see Section 5.

Subject access right

The purpose of subject access rights is to allow individuals to obtain a copy of their own personal data, confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. The University must respond to all requests for personal information within one month. Any member of staff receiving a request from an individual for their own personal information should consult the relevant guidance on the Records Management website:
Dealing with Subject Access Requests

Right to erasure (to be forgotten)

Data subjects have the right to request that their personal data be removed from all the systems of the University if certain requirements are met. These requirements are:

- The University does not need to keep the data anymore in relation to the purpose for which they were originally collected/processed.
- The data subject withdraws consent for the processing to which they previously agreed

- The subject uses their right to object to the data processing (possible where the legal basis is either 'public task' or 'legitimate interest').
- The University is processing the data unlawfully (i.e. in breach of the GDPR and/or the DPA)
- The personal data must be erased in order to comply with a legal obligation.
- The data subject was a child at the time of collection.

This means that if the legal basis for processing the data is 'performance of a contract' or 'legal obligation', and processing is fully lawful, the request must be refused.

However, even if the request meets one or more of these requirements, there are still a number of exemptions when the University will not have to comply. Thus, data might not have to be erased if any of the following apply:

- The personal data are processed to exercise the right of freedom and expression (e.g. journalism, artistic work)
- The personal data are needed for legal compliance
- There are reasons of public interest in the area of public health
- The data are processed and stored for scientific, historical research or archiving purposes in the public interest
- The data are needed for a lawsuit

If you receive a request for data erasure, immediately contact your local Data Protection Champion. A list of the Data Protection Champions can be found here:
Data Protection Champions (link to be added)

Right to rectification

Data subjects are entitled to request that their personal data are rectified if the data are inaccurate or incomplete. If you receive such a request, you must comply within one month. Should complying with the request for rectification be particularly complex, then the time can be extended to two months.

If you have shared the personal data with third parties, or within the University, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

Right to portability

The right to data portability gives data subjects the possibility to request that the University pass their personal data on to a third party of their choice and allow that third party to import the data automatically.

Data subjects have this right if certain requirements are met. These requirements are:

- The individual has provided the personal data to the University, and
- The legal basis for processing is 'consent' or 'performance of a contract', and
- The processing is carried out solely by automated means with no human involvement.

If these requirements are met, then the data must be provided in a structured, commonly used and machine readable form.

If you receive a request for portability, immediately contact your local Data Protection Champion. A list of the Data Protection Champions can be found here:
Data Protection Champions (link to be added)

Right to object

Data subjects have the right to object to the University processing their personal data if certain requirements are met. These requirements are:

- The legal basis for processing is 'legitimate interest' or 'public task';
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

When data subjects have an objection on "grounds relating to his or her particular situation", then you must stop processing the personal data unless:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject; or
- The processing is for the establishment, exercise or defence of legal claims.

The right to object to profiling for direct marketing is an absolute right. That means that for such objections, data subjects will not need to provide any grounds relating to their situation, and the University is not allowed to override the objection. .

If you receive a notification of an objection to processing, immediately contact your local Data Protection Champion. A list of the Data Protection Champions can be found here:
Data Protection Champions (link to be added)

Right to restrict processing

Data subjects have a right to 'block' or suppress processing of their personal data, i.e. to request that you immediately stop processing their personal data in any way except to store it. This right applies only if one of these requirements are met:

- A data subject contests the accuracy of the personal data - you should restrict processing until you have verified the accuracy.
- A data subject has objected to the processing (see above), and you are considering whether the University's legitimate grounds override those of the data subject.
- Processing is unlawful, the data subject does not trigger the right to be forgotten, but requests restriction of use instead.
- You no longer need the personal data and would delete them in accordance with the retention schedule, but the data subject requires the data for a lawsuit.

Right to object to automated processing and profiling

The prohibition

There is a clear prohibition regarding decisions based solely on automated decision making and on profiling which produce *legal effects* or which *similarly significantly affect* an individual.

"Legal effects" have an impact on a data subject's legal rights, affect a data subject's legal status or their rights under a contract.

"Similarly significantly affects" means the processing must be more than trivial and must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly influence the circumstances,

behaviour or choices of the data subjects concerned. At its most extreme, the decision may lead to the exclusion or discrimination of data subjects.

There are three exceptions from that prohibition, and that is where automated decision-making:

- is necessary for the performance of or entering into a contract;
- is authorised by law; or
- is based on the data subject's explicit consent

Data subject rights

Even where the three exceptions apply and automated decision-making and profiling can be used, data subjects still have rights. They can still object to the automated processing and request that a human being become involved and reconsider the decision.

Also, data subjects have the absolute right to object to profiling, as seen above under 'the right to object'.

If you believe that you are using automated processing or profiling, contact the DPO at dpo@ed.ac.uk.

12 – Research

Research under the GDPR changes as regards the legal basis for processing research data. Ethics consent to participate in a study remains unchanged, as does the requirement for a Participant Information Sheet.

The legal basis for processing personal data, which used to be consent, has now been replaced by 'public task' and by 'necessary for scientific or historical research purposes in accordance with safeguards'. These safeguards are what is currently considered good practice:

- The minimisation principle – use only the absolute minimum of personal data required for your purpose
- Anonymise personal data if you can
- If you cannot anonymise, wherever possible, pseudonymise all personal data
- Store the data securely

Furthermore, you must be able to prove that research is in the public interest. Possible evidence includes one of the following:

- Your research must be proportionate,.e.g. it must not be more intrusive into participants' privacy than necessary, you must not collect more data than you actually need for your study
- Your research is subject to a policy research governance framework, e.g. the UK Policy Framework for Health and Social Care Research
- Research Ethics Committee (REC) review (does not have to be a European REC)
- Peer review from a research council

- In the case of medical research, Confidentiality Advisory Group (CAG) recommendation for support in England and Wales or support by the Public Benefit and Privacy Panel for Health and Social Care in Scotland

When you have the necessary safeguards in place, the rights of research participants are restricted. The following rights will not apply where it would prevent or seriously impair the achievement of the research purpose and where your legal basis is public interest plus the additional research-related legal basis for special categories:

- The right to rectification
- The right to restrict processing
- The right to object to processing
- The right to erasure (right to be forgotten)

More detailed guidance can be found here:
Research under GDPR (link to be inserted)

13 – Student Research

Students will conduct research as part of their undergraduate work (Honours dissertation) or as part of their postgraduate work (dissertations for a Masters Degree or a Doctorate). Students will remain the data controller and as such responsible for their research until they submit their dissertation. At that time the University becomes a joint data controller with the student.

The only exception to this is where a student processes personal data whilst working on a project led by a university research group. In this case, the student and the University are both data controllers from the outset.

14 – Automated Decision-Making

Assessment marking

The University does not use solely automated decision-making when marking exams. Even multiple choice tests that may be checked and marked by automated means do not fall under the definition of solely automated decision-making, as the exam has been set by a human being, the correct answer has been determined by a human being and the automation applies only to checking the given answers against the correct one.

Learning analytics

When using learning analytics, the University will take the following approach as regards the legal basis:

- Use legitimate interests as the legal basis for the processing of non-sensitive personal data for analytics
- Obtain consent for processing of sensitive personal data (which, under the GDPR, will be called “special category data”)
- Obtain consent to make interventions directly with students on the basis of the analytics.

In accordance with the rights set out above under section 11, individuals can object to the processing where legitimate interest is the legal basis. For the situations where consent is required, that consent can either be withheld or withdrawn at any time.

15 – Data Protection by Design and Default

Data protection by design (also called 'privacy by design') is an approach to projects and initiatives involving personal data that is intended to incorporate data protection compliance from the start rather than considering it as an after-thought.

Thus, the University is required to implement the appropriate technical and organisational measures both at the time when the methods and ways of processing personal data are determined and also at the time of the processing itself. In addition, the University will need to ensure that, *by default*, only personal data that are necessary for each specific purpose are actually processed.

Examples for technical and organisational measures are:

- Data minimisation
- Additional layers of encryption
- Data retention limits
- Restricted access
- Anonymization and pseudonymisation
- Encryption, hashing, salting

All staff and agents of the University are required to apply the data protection by design principles when developing a new project or reviewing existing projects that involves the use or storage of personal data. The guidelines below explain the types of project when this might be relevant, what data protection by design is and what measures can be put in please to protect personal data.

Data Protection Impact Assessments

One important measure that is expressly listed in the GDPR as a mandatory requirement is conducting a Data Protection Impact Assessment (DPIA) for projects or initiatives that may have a negative impact on data subjects' privacy. A DPIA is a type of risk assessment whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders.

A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also if there is a change to the risk of processing for an existing project a review should be carried out.

The DPIA will then continue to assess privacy impacts throughout the lifespan of the project. Examples of the types of projects where a DPIA needs to be considered include:

- Building or buying new software or IT systems for storing or accessing personal data
- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A new surveillance system such as CCTV

- Using personal data for new purposes such as a new database which consolidates information held by separate unrelated parts of the University

In addition to meeting legal requirements, taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.

A template and guidance on how to conduct a DPIA can be found here:
Data Protection Impact Assessment and Guidance

Pseudonymisation

Pseudonymisation is a privacy-enhancing technique; it is a process rendering data neither completely anonymous nor directly identifying. With pseudonymisation you separate personal data from direct identifiers so that linkage to an identity is no longer possible without the additional information that is held separately. It is important to note that pseudonymised data is not exempt from the GDPR and the DPA.

If you pseudonymise a research dataset by keeping the data and the identifiers separate and send the pseudonymised data to another University without also sending the identifiers, then the other University will process anonymised data. You, however, will still process personal data as you can still at any time re-identify individuals.

Under certain circumstances, pseudonymised data can be exempt from data subject rights. This exemption, however, applies only if you are able to demonstrate that you are not in a position to identify the data subject anymore, e.g. when you destroy the identifiers but you know that they still exist elsewhere. You will then not be required to comply with subject access requests, as the GDPR does not require a controller to hold additional information for the sole purpose of complying with such requests. If, however, data subjects provide you with the additional information you would require to re-identify them in the data set, they must be permitted to exercise their rights.

Anonymisation

Anonymised data means that all identifiers have been irreversibly removed from data subjects and they are no longer identifiable in any way. In this case, the GDPR and the DPA do not apply any longer – the data is no longer personal. However, with the advances in modern technology, re-identification will become easier.

16 – Direct Marketing

Direct marketing includes the advertising or marketing of commercial products or service as well as fundraising, and includes all messages promoting an organisation such as promoting University events or opportunities for students.

Direct marketing covers all forms of communication, such as marketing by letter, telephone, email and other forms of electronic messages.

Finding the correct legal basis for direct marketing is very important. The law distinguishes between direct marketing using electronic means and non-electronic means. Currently, ‘electronic means’ covers the use of email and text messaging.

For marketing by letter and telephone, the GDPR applies and your legal basis can be ‘legitimate interest’ – you will not need consent.

The Privacy and Electronic Communications Regulations 2003 (PECR) regulate the use of electronic communications such as email or text messaging as a form of marketing. PECR is due to be replaced shortly by a new ePrivacy Regulation (ePR).

Electronic marketing to private individuals can only be done with consent as the legal basis. Consent must be a positive action, such as signing up to a newsletter or ticking a box and any direct marketing messages should only be sent to those people who have in fact opted in. One exception to the need to obtain prior consent is the so-called 'soft opt-in', which is based on 'legitimate interest'. Soft opt-in can be used in situations where you have a pre-existing commercial relationship with the individual.

The full guidance on direct marketing can be found here:

Direct Marketing under Data Protection Law (link to be inserted).

17 – Data Protection Breaches

A data protection breach is defined in GDPR to mean:

> "a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The GDPR imposes a requirement that certain data protection breaches are reported to the Information Commissioner's Office within 72 hours of the University becoming aware of the breach.

While the University makes every effort to avoid data protection breaches, it is possible that mistakes will occur on occasions or things will happen that are beyond the University's control. This section of the Handbook sets out the procedures to follow if a personal data incident has occurred. All individuals who access, use or manage the University's information are responsible for following these guidelines and for reporting any data protection incidents that come to their attention.

A personal data incident can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

It is the responsibility of any staff, student or other individual who discovers a personal data incident to report it immediately the IS Helpline on:

0131 651 5151 or IS.Helpdesk@ed.ac.uk

IS Helpline will require information from you about the nature of the breach, i.e. what happened, and whether any personal data was involved. This could be the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

IS Helpline will then forward the incident either to Information Security or to the Data Protection Officer and Records Management.

The Data Protection Officer will determine whether the incident constitutes an actual data protection breach and will act accordingly to help contain the incident and, where necessary, assist with notifying the affected data subjects. The Data Protection Officer will also, where required, notify the Head of College, School or Department, the University Secretary and the Information Commissioner's Office.

The Data Protection Officer will keep a record of all data protection incidents and breaches including the actions taken to mitigate the breach and the lessons learnt.

18 – Mailing lists

Privacy notices

Whether your communication is internal or external, electronic or in paper format, you must always ensure that recipients receive a privacy notice, through either a link or the entire privacy notice in the footer of all emails, and a link or the entire privacy notice included in all letters sent out.

External mailing lists in paper format

If your external mailing list is used to send communications in paper format, you will not need to obtain consent. Instead, your legal basis is 'legitimate interest'. You must, however, provide recipients with the opportunity to easily and effortlessly opt out of receiving the communication in every letter.

External mailing lists in electronic format

Business-to-business

If you send emails to business contacts, i.e. individuals who can be considered as representatives of their company, organisation or institution (e.g. students or academics from another university), you can rely on legitimate interest. However, you must provide the option to opt out in every communication.

Private individuals

If you send emails to private individuals, then you must have obtained consent. If an existing mailing list contains exclusively or mostly of private individuals who have not subscribed but have been added to the list, then you must request consent and remove those who don't reply from the list. After an appropriate period of time, consent must be refreshed. Always provide the option to opt out in every communication.

Mixed lists

If your mailing list contains both B2B contacts and private individuals and you have not obtained consent from the private individuals, conduct a risk assessment to

determine whether continuing to send emails is likely to cause offence or distress or whether receiving the emails is in the individuals' interest and/or to their benefit.

Internal mailing lists in electronic format

For essential business mailing lists with information such as changes in lecture theatre for students, information lack onf heating or power failure in certain buildings, subscription is mandatory and an option to unsubscribe cannot be given and the legal basis for these emails is 'contractual obligation'.

For non-essential mailing lists about, for example, events in a School or career opportunities for students, staff members and students are considered to be business contacts, and the legal basis for these emails is 'legitimate interest'. Always provide the option to opt out in every communication.

The full guidance on mailing lists can be found here:

Mailing lists and data protection (link to be inserted)

19 – CCTV

For CCTV systems, two types must be distinguished:

- Cameras that record
- Cameras that only show live footage but don't record

Only cameras that record fall under the GDPR and the Act.

However, even if cameras that only show live footage are not subject to the GDPR and the Act, it is good practice to include them when complying with the fairness and transparency requirements, i.e. when displaying appropriate signage where cameras are in use.

Only for cameras that record are you required to have a legal basis. This legal basis depends on the purpose for the cameras.

- If the cameras are in a high-security laboratory, you will be able to rely on 'legal obligation'.
- In all other locations, your legal basis will be 'necessary for legitimate interest', as the cameras will be intended to assist with general safety and security.

Individuals whose images are recorded have a right to view the images of themselves and to be provided with a copy of the images.

Further guidance can be found in the CCTV policy:
CCTV Policy (link to be inserted)

20 – Photography

Whenever individuals can be identified by their image, data protection legislation applies. In these situations, the rights of the individuals in the collection and use of their photographs must be respected – they must be informed when an identifiable image of them will be or has been captured, and consent must be obtained before the image is used in any way.

Taking photographs

Photographs of individuals

You must obtain consent when taking photographs of a specific person that you might want to publish on the internet. Tell them what you intend to do with the photographs, including that they will be published on the Internet.

Photographs of posed groups

When taking photographs of a group of people posing for the picture you must obtain the consent of each member of the group. Tell them what you intend to do with the photographs, including that they will be published on the Internet.

Photographs of crowds

If crowd shots are taken during an event and an individual is not identifiable, then it is not necessary to obtain consent to take, display or publish the photo, rather, the legal basis is legitimate interest. This applies to any individuals, students and staff whose images are incidental detail, such as in crowd scenes for graduation, conferences and in general campus scenes.

You must, however, include notices at the event informing attendees of the fact that photo are being taken so they have the opportunity to opt out.

Photographs of children

If taking photographs of children, you must obtain consent from a parent or guardian. This may be written or verbal depending on the circumstances, see the guidance above.

Using photographs

ID photographs

ID photographs can always be used for security purposes and to identify individuals such as using these photographs for identifying students during assessments and exams. This is covered by the legal basis “necessary for performance of a contract”.

Intranet/wiki

Use of staff and mainly postgraduate students’ photographs on the intranet or a wiki with restricted access alongside their contact details is covered by the legal basis “necessary for a legitimate interest” as these photographs are required for the effective operations of university business. Individuals can object to this by advising their line manager or supervisor of studies if they have a legitimate reason why their photograph should not be published.

External facing websites

If photographs of individuals are to be published on an external facing website, consent will be required.

The full guidance on photography can be found here:
Photography guidance (link to be inserted)

THE UNIVERSITY of EDINBURGH

J

UNIVERSITY EXECUTIVE

14 May 2018

Draft University Risk Register 2018/19

Description of paper

1. This paper presents an initial update of the University Risk Register (URR) for 2018/19 (summary version attached as Appendix) for the University Executive's consideration and comments.

Action requested/Recommendation

2. The University Executive is asked to consider this draft of the URR and provide suggestions, comments and recommendations.

Paragraphs 3 - 6 have been removed as exempt from release due to FOI.

Next steps & Communication

7. Taking into account any comments, the URR will be forwarded to the Audit & Risk Committee meeting on 31 May 2018 for consideration and recommendation to Court for approval on 18 June 2018.

Consultation

8. The draft URR was considered by Risk Management Committee at its meeting on 7 May 2018.

Further information

9.

Author
Kirstie Graham, Court Services
May 2018

Presenter
Hugh Edmiston
Director of Corporate Services

Freedom of Information

10. This paper is closed.

THE UNIVERSITY of EDINBURGH

K

UNIVERSITY EXECUTIVE

14 May 2018

Report from Fee Strategy Group

Description of paper

1. This paper sets out the recommendations from the Fee Strategy Group meeting of 29 March 2018 which the University Executive is asked to approve or note as appropriate. The paper also sets out action taken by the Chair since the last FSG report to the University Executive on 12 March 2018.

Action requested/Recommendation

2. The University Executive is asked to consider and approve unregulated tuition fee inflation and rate proposals outlined in paragraphs 9, 11, and 13 and to note routine fee approvals for 2018/19 taken by the Chair of the Fee Strategy Group (paragraph 14).

Paragraphs 3 - 15 have been removed as exempt from release due to FOI.

Risk Management

16. The proposals for fee rates included in the paper takes into account the University's appetite for financial risk as well as student experience and reputation.

Equality & Diversity

17. Equality and diversity issues are considered as part of the on-going monitoring of fee levels by the Fee Strategy Group and its Secretary. We do not consider that an EIA is required.

Next steps & Communication

18. Once endorsed, the fees will be published by Scholarships and Student Funding Services and on School and other websites as well as in promotional literature.

Consultation

19. The paper has been reviewed by Tracey Slaven, Deputy Secretary Strategic Planning

Further information

20. Further information can be obtained from Peter Phillips, Deputy Director of Planning, GaSP (tel: 50-8139, email: Peter.Phillips@ed.ac.uk)

21. *Author*
Jennifer McGregor
Governance and Strategic Planning
4 May 2018

Presenter
Tracey Slaven
Governance and Strategic Planning

Freedom of Information

22. This paper should be closed and disclosure would substantially prejudice the commercial interests of the University until the fee rates are published.