2

(which may at times exceed those of College policies with respect to
storage or security requirements ² e.g. for funded research).

5. This policy is approved by the College Council and will be reviewed
annually. Council remains responsible for ensuring appropriate resources are
in place to achieve compliance with data protection law in line with an
appropriate overall risk profile.

Obligations of the College

6. The College upholds data protection law as part of everyday working
practices, by:

 ensuring all personal information is managed appropriately through this policy;
 understanding, and applying as necessary, the data protection principles when
processing personal information;
 understanding, and fulfilling as necessary, the rights given to data subjects
under data protection law;
 understanding, and implementing as necessar\, the College·s accountability
obligations under data protection law; and
 the publication of data protection statements outlining the details of its
personal data processing in a clear and transparent manner.

Further details about the above may be found in the Annex on page 4.

7. The College shall appoint a statutory data protection officer, who will work
with the College Data Protection Lead to:

 monitor and audit the College·s compliance with its obligations under data
protection law, especially its overall risk profile, and report on such annually to
the College;
 advise the College on all aspects of its compliance with data protection law;
 act as the College·s standard point of contact with the Information
Commissioner·s Office with regard to data protection law, including in the case
of personal data breaches; and
 act as an available point of contact for complaints from data subjects.

8. The College shall otherwise ensure all members and staff are aware of this
policy and any associated procedures and notes of guidance relating to data
protection compliance, provide training as appropriate, and review regularly
its procedures and processes to ensure they are fit for purpose. It shall also
maintain records of its information assets.

9. Individual members and staff are responsible for:

 completing relevant data protection training, as advised by the College;
 following relevant College policies, procedures and notes of guidance;
 only accessing and using personal information as necessary for their contractual
duties and/or other College roles;

3

 ensuring personal information they have access to is not disclosed unnecessarily
or inappropriately;
 where identified, reporting personal data breaches, and co-operating with
College authorities to address them; and
 only deleting, copying or removing personal information when leaving the
College as agreed with the College and as appropriate.

Non-observance of the responsibilities in paragraph 9 may result in
disciplinary action against individual members or staff.

10. The obligations outlined above do not waive any personal liability for
individual criminal offences for the wilful misuse of personal data under
data protection legislation.

Last updated: 8 May 2018

Data Protection statements, advice for Data Subjects and other documentation
related to Data Protection may be found on the College Data Protection page
Other resources referred t1tes mn
BT
/F4 11.04 Tf
1/F4 r6d0 0 1 72.0.8b
[(1teA1 72n
BT
/F62.1 09n)-3(-2(a)-02r 4(a)-4(t)-3(a)-4(Pr)8(o)-2(t)-3(e)5(c)-4(t)-3(i)5(o)-2(n)-3(p)8(a)-4(ge)] TJ

5

 the right not to be subject to a decision based solely on automated decision-making using their personal data.

Accountability

The College is required under law to:

 comply with data protection law and hold records demonstrating this;
 implement policies, procedures, processes and training to promote ´data
protection b\ design and b\ defaultµ;
 have appropriate contracts in place when outsourcing functions that involve
the processing of personal data;
 maintain records of the data processing that is carried out across the College;
 record and report personal data breaches;
 carry out, where relevant, data protection impact assessment on high risk
processing activities;
 cooperate with the Information Commissioner·s Office (ICO) as the UK
regulator of data protection law;
 respond to regulatory/court action and pay administrative levies and fines
issued by the ICO.