

# BLAVATNIK SCHOOL OF GOVERNMENT – IT ACCEPTABLE USE POLICY

## General Principles

This policy governs the use of Information Technology equipment and services supplied by or on behalf of the Blavatnik School of Government.

As an International teaching and research organization, the Blavatnik School of Government holds as a key principle that easy, open and confidential access to Information Technology and Communication tools and services should be given without unreasonable monitoring or oversight.

In return for access to systems, you are asked to use those systems responsibly and to respect the principles and reputation of the School and University, to treat other users with respect and of course to comply with UK and international law.

This policy is local to the BSG; it is a summary of central University IT policies and best practices. The policy should be seen as supplementary to, and not replacing any acceptable use and Information Security policies or statutes of the University of Oxford. Related policies are listed and linked in the references at the end of this document.

## Scope

The scope of this policy includes any product or service provided directly by the School, the University of Oxford, or contracted third parties and includes, but is not limited to:

- Computer hardware, including School supplied mobile phones and tablet computers.
- Software supplied by or on behalf of the school.
- Access to the School's wired and wireless network.
- Access to the University of Oxford network and the public internet.
- Storage of computer files and data, including the use of backup services.
- Email and other communication systems supplied by the University of Oxford.
- Websites hosted by or on behalf of the School or University.

Access to these systems and services is authorised for users on the condition that they comply with the policies described in this document.

## Acceptable Use

ICT services are supplied by, or on behalf of the Blavatnik School of Government to:

- Further the objectives of the Blavatnik School of Government
- Carry out Academic Research
- Carry out Teaching
- Directly or indirectly support any activities listed above.

Under University policy users have no right to use systems or services for personal use. However permission is given for users to access services (as listed in the scope section) for personal use as long as they are not:

- In breach of any of the Unacceptable Use criteria listed below.
- Likely to cause material or reputational harm to the School
- Likely to make the School liable for additional financial costs or liabilities.

## Unacceptable Use

Users may not use ICT services (as listed above) to:

- Carry out any activity that may reasonably be regarded as unlawful or potentially so.
- Create, store or transmit, or cause the transmission of offensive, obscene or indecent images, data or data capable of being resolved into obscene or indecent material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation, storage or transmission of material with the intent to defraud.
- Creation, storage or transmission of defamatory material.
- Creation, storage or transmission of material such that this infringes the copyright of another person, this includes the sharing of copyright material on peer-to-peer file sharing networks.
- Deliberate unauthorised access to IT or networked facilities or services.
- Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
  - corrupting or destroying other users' data;
  - violating the privacy of other users;
  - disrupting the work of other users;
- Introduce a virus or other malicious software into the network.
- Waste staff effort or computer or network resources.
- Carry out commercial activity, except where agreed by the School's Senior Management Team.

## Exceptions for Academic Research

There is an understanding that, as part of a research project sponsored by the School, Academic Staff may need to access material that is seen as offensive or obscene. Any member of Academic Staff who feel that their research may bring themselves into conflict with this policy should apply to the Dean for a confidential waiver.

It should be noted that there is no provision for any staff to access unlawful material.

## Responsibilities of IT Support Staff

IT Staff from the Blavatnik School of Government ICT team and other authorised staff from the University of Oxford IT Services or directly contracted third party support teams have privileged access to User data.

ICT Staff are bound by the Acceptable and Unacceptable use policies stated above, with the following addendum:

Access to User and System data and metadata is given solely for the purposes of:

- Operating and delivering technical services, for example monitoring network throughput, operating data backup and recovery tools.
- Providing end user support.
- Investigating potential breaches of Information Security or Acceptable Use policies of the Blavatnik School of Government or University of Oxford.

IT Staff are not permitted to:

- Access User data or metadata except for the express purposes listed above.
- Ask for, infer or accept personal access credentials such as passwords or any other key or security token.

Normally permission will be sought from the user before attempting to access their data.

If it is not possible or appropriate for staff to contact that user, permission will be obtained from the Dean, Vice Dean or Chief Operating Officer of the Blavatnik School of Government.

## Investigation and Remedy

Potential breaches of this policy should be made in the first instance to the Blavatnik School of Government Head of ICT, HR Manager or a member of the Senior Management Team.

Depending on the nature of the potential breach investigations will take the following form:

- Technical breaches which impact information security or the reliable delivery of services to other users in the School, or across the wider Academic

Network will result in the removal of systems from the network while the breach is investigated.

- Breaches involving a potential conflict with the principles of academic freedom or freedom of speech will be escalated to a Faculty member of the Senior Management Team.
- If IT Staff have reasonable grounds to believe that a serious breach of this policy has occurred in contravention of UK law, the potential breach will be escalated to a member of the Senior Management Team and the police will be asked to investigate.

## References

Document	Location	Author	Date retrieved	Version retrieved
Regulations Relating to the use of Information Technology Facilities	<a href="http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml">http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml</a>	ICTC	7 <sup>th</sup> July 2016	ICT Regulations 1 of 2002.
JANET Acceptable Use Policy	<a href="https://community.jisc.ac.uk/library/acceptable-use-policy">https://community.jisc.ac.uk/library/acceptable-use-policy</a>	JISC	7 <sup>th</sup> July 2016	12

Version	Author	Date	Reason
0.1	M Treavis	07/07/16	Initial policy for comment.
0.2	M Treavis	06/10/16	Draft policy for approval.
1.0	M Treavis	12/10/16	Published – approved by SMT