

Acceptable use of IT Policy

Responsible Person	John Joannou, Head of Technology
Approving Body	Academic Board
Date of Approval	November 2020
Date of Effect	30 th November 2020
Last Updated	
Next Review Date	July 2021
Queries	john@metfilm.co.uk

Related Polices:

- MetFilm Data Protection Policy
- MetFilm Equal Opportunity & Diversity Policy
- Safeguarding Policy
- Student Disciplinary Policy
- MetFilm School Harassment and Bullying Policy
- MetFilm School Complaints Policy

1. Definitions

- 1.1. "IT Systems" includes central services as provided by MetFilm such as e-mail, networks, internet access, computers, computing equipment and mobile devices, personally owned computers and devices when connected to, or accessed from or via MetFilm facilities,
 - use of remote networks and services, when accessed from or via MetFilm IT Systems;
 - all programmable equipment; any associated software and data, including data created by persons other than users, and the networking elements which link MetFilm Systems.
- 1.2. "users" includes students, staff, workers, honorary title holders, visiting academics and any other person authorised to use MetFilm's IT Systems.
- 1.3. "connected to" means connected either physically or virtually.
- 1.4. "files" include data and software but do not include 'physical' or 'paper' files.

2. Purpose and scope

- 2.1. This policy sets out the standards which apply to all users in their use of MetFilm's IT Systems.
- 2.2. Our IT Systems are provided to users as part of their equipment for work and/or study, namely for learning, training, research, development and administrative purposes. There are, however, risks involved in the use of the IT Systems.

Inappropriate use of the Internet or e-mail could damage the operation, business or academic activities or reputation of MetFilm. Examples of such risks include:

- claims brought against MetFilm because the reputation of other individuals or organisations has been damaged;
- unauthorised disclosure of information, which is confidential to MetFilm or its staff and/or students;
- infringement of copyright, licenses and other rights in MetFilm's and other parties' material (which includes infringement arising from the use of material without the permission of the creator);
- harassment and discrimination claims being brought against MetFilm (caused by offensive or other inappropriate material);
- entering into contracts on behalf of MetFilm by mistake;
- inadvertent breach of contract by MetFilm;
- the introduction of viruses and/or malware to MetFilm's IT Systems.

- 2.3. This policy is designed to prevent these and other problems and therefore you are expected to be familiar with and comply with the contents of this policy. Users should seek advice and clarity if unsure about whether anything they are considering undertaking might breach this policy.
- 2.4. Failure to adhere to this policy may result in disciplinary action. Please refer to the student disciplinary procedures for further details.
- 2.5. This policy applies to all users in whatever location they are working whether or not on MetFilm premises when interacting with MetFilm supplied systems and resources.
- 2.6. This policy considers the current legal position, but users should be aware that it will continue to change, often at great pace. For this reason, all users must ensure that they update themselves regularly with this policy. In the event of a conflict between this policy and the law, the law will prevail.

3. Bring Your Own Device (BYOD)

- 3.1. MetFilm recognises the benefits that can be achieved by allowing users to use their own electronic devices. MetFilm must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing.
- 3.2. Users who make use of BYOD must take responsibility for their own device and how they use it. They must:
 - familiarise themselves with their device and its security features so that they can ensure the safety of MetFilm information as well as their own information;
 - invoke the relevant security features;
 - maintain the device themselves ensuring it is regularly patched and upgraded.
- 3.3. All users using BYOD must take all reasonable steps to:
 - prevent theft and loss of data;
 - keep information confidential where appropriate;
 - maintain the integrity of data and information, including that on campus;
 - Take responsibility for any software they download onto their device.
 - Ensure all passwords and security conforms to MetFilm guidelines.
- 3.4. Where it is essential that information belonging to MetFilm is held on a personal device it should be deleted as soon as possible once it is no longer required.
- 3.5. Users should report the loss of any device containing MetFilm data (including email) or any security breach to the Operations and IT departments in accordance with the Data Protection policy.

4. Use of Cloud Based and Portable Storage.

- 4.1. MetFilm utilises Microsoft 365 cloud storage solutions.

- 4.2. No MetFilm data should be stored (particularly confidential or personal information) on any device outside of MetFilm with the exception of devices meeting the security requirements herein.
- 4.3. Use of any external or remote storage systems must conform to MetFilm data storage policies as outlined in this document. This includes;
 - use of appropriate passwords and security mechanisms;
 - that all instances of use are communicated and approved by line managers;
 - that all data processed on these devices is done so in line with the MetFilm Data Protection Policy.

5. Disabled Students and Staff

- 5.1. The IT systems in use are regularly reviewed to ensure they are Inclusive. Please contact MetFilm Students Services for further information on the services we provide to disabled people.

6. Usernames and Passwords

- 6.1. You should keep your password secure at all times and must not reveal your password to anyone else. The use of another person's username and/or password, with or without their permission will be dealt with under the Student Disciplinary Procedures as appropriate.
- 6.2. All users must register the Microsoft Self Service Password Reset (SSPR) function for their Microsoft 365 account. This allows the user to reset their password via a secondary device, alternate mail account or security questions.
- 6.3. Your password must conform to the following.
 - Passwords must be at least 8 characters long
 - Passwords cannot contain your name or user name
 - Accounts are locked after a set number of failed attempts (10 for Office 365). They are reset Via Self Service Password Reset mechanisms for Office 365 accounts or by the MetFilm IT Support Team and Student Services Team for other MetFilm accounts.
 - Your password must include characters from 3 of the following 4 categories:
 - upper case letters;
 - lower case letters;
 - numbers;
 - special characters ` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /

Further advice and guidance on selecting and maintaining your password can be found at <https://computing.which.co.uk/hc/en-gb/.....How-to-create-secure-passwords>

7. Acceptable Use of MetFilm Systems

- 7.1. As a general rule MetFilm IT Systems should be used solely for MetFilm academic and business purposes. Limited use of the IT Systems for personal reasons is acceptable provided that:

- the usage is minimal
- the usage does not affect or interfere with the operation, business or academic activities of MetFilm in any way;
- you do not enter into any contracts or commitments in the name of or on behalf of MetFilm;
- the usage does not commit MetFilm to any costs;
- the usage conforms to the guidelines set out in this policy.

7.2. Never send e-mails or access the Internet under a name other than your own name.

8. Offensive and other inappropriate material

- 8.1. You may not use the IT Systems if the purpose or effect of such use is the downloading, viewing, listening to, posting, or circulation of information, e-mail messages, images, audio files or other data which are or which MetFilm may consider to be offensive or inappropriate. This will include material which is or could be perceived as being:
- obscene or pornographic; or
 - racist, sexist or discriminatory or offensive in any other way (including, but not limited to, on grounds of disability, sexual orientation, age, religion or other protected characteristics); or
 - politically extreme; or
 - defamatory; or
 - untrue, abusive or malicious; or
 - bullying or harassing; or
 - an infringement of the rights of any other person anywhere in the world; or
 - otherwise objectionable.
- 8.2. MetFilm has a duty under the Counter-Terrorism and Security Act (2015), to prevent people being drawn into terrorism. To meet this duty MetFilm's systems must not be used to create, access, transmit or download inappropriate materials as defined under the Prevent legislation. MetFilm reserves the right to monitor, alert and report attempted access to, or dissemination of, such inappropriate material.
- 8.3. The definition of extremist material will be governed by Home Office definitions within the Prevent Guidance (2015).
- 8.4. The question of what constitutes offensive material is not one for the sender to determine - it is the effect on the recipient which is important. You should not therefore pass on any material which even risks causing offence to any recipient. For this reason, the circulation of e-mails and other materials containing strong language or offensive jokes is not permitted.
- 8.5. You must report to IT Support (who will treat this concern with sensitivity) any person you know or reasonably suspect to be acting in breach of this section of this policy and take immediate steps

to prevent continued access to, or distribution of material from sites, or the sending of e-mails containing offensive or inappropriate material as described in paragraph 8.1.

- 8.6. If you feel that you are being harassed or offended in any way by the use of the facilities by any other student or member of staff (or even by people outside MetFilm), whether or not such harassment or offence is intentional, you should report in accordance with MetFilm Schools Complaints Policy with reference to the MetFilm School Harassment and Bullying Policy.
- 8.7. MetFilm reserves the right to monitor all incoming internet traffic by scanning MetFilm's systems for such material and where there is a systematic or deliberate pattern of misuse, this will lead to formal action under our student disciplinary procedures.
- 8.8. In the event that a user is found to have accessed or received such materials, their IT usage may be examined in detail to ascertain whether usage is part of a systematic pattern of misuse. No disciplinary action may be taken if the misuse is not systematic, as we recognise that users may receive occasional unsolicited messages or access an internet site in error. However, the user must immediately notify IT Support upon receipt of or upon accessing any such material.
- 8.9. In the rare event that visits to obscene or pornographic web sites are required for legitimate academic purposes, permission for such usage must be sought in advance and in writing from relevant Course Leader, with decisions copied to itsupport@metfilmschool.ac.uk
- 8.10. The receipt and/or distribution of such material including the circulation of it to another user or users may also be a criminal offence and MetFilm reserves the right to report any such incidents to the Police.
- 8.11. MetFilm reserves the right to prevent access to materials it feels are inappropriate and also where MetFilm is required to do so by Law, Policy or Statutory duty.

9. Acceptable Use of the internet

- 9.1. Do not download software, programs, videos, music or other content (even if free) from the web onto MetFilm's IT Systems unless such download is necessary in the proper performance of your duties if you are staff member and even then, do not do so without the prior written/e-mail permission of the IT Support Team. This prohibition extends to screen-savers and games.

10. Acceptable Use of e-mail

- 10.1. You are reminded that e-mails are a form of written communication which is permanent, and which may be read by any member of the public. You should therefore always consider whether it is appropriate to use e-mails for the particular communication envisaged. Please note that we may be required to disclose e-mail messages in legal proceedings relating to their subject matter and that the deletion of a message or file may not fully eliminate it from the IT Systems.

- 10.2. If it is necessary to send sensitive or confidential information by email, then care should be taken to provide a reasonable level of protection. You should be as careful about the content of e-mails as you would be with letters. Consider in every case whether the content of an e-mail would reflect well on MetFilm and, in particular, you should make sure that:
- all contents are accurate and appropriate for dissemination by e-mail;
 - disparaging or unduly critical comments are avoided;
 - you have the authority to communicate the particular information on behalf of MetFilm.
- 10.3. The language of any e-mails you send should be in accordance with the standards of any other written communications and at all times the language used should be appropriate to formal business communications. You should under no circumstances use e-mails to spread gossip or similar information and the prudent test would be for you to write in e-mail form only such matters (and in such language) as would be considered suitable for a letter.
- 10.4. E-mail can sometimes be used as a medium for bullying and intimidating other people. This will not be tolerated. If you are unhappy about something please discuss the matter with your course leader, personal tutor or a member of Student services.
- 10.5. If you generate or forward e-mails to others, you must be very clear as to the intended recipient. The inadvertent dispatch of material to a collective user group, for example, is no different from sending it individually to all those within that group.
- 10.6. Students should not accept or open any file received as an e-mail attachment if you are in any doubt as to its source, as you may spread a virus or malware or compromise you account information. If in any doubt, contact IT Support.

11. Websites

11.1. We have a websites on the Internet, currently situated at

- metfilmschool.ac.uk
- metfilmschool.de
- screenspace.ac.uk
- metfilmproduction.co.uk
- metfilmsales.com

Your use of the website is subject to the terms of this policy and to any terms of use posted from time to time on the website.

11.2. We own or are licensed to use all copyright, other intellectual property rights in and pertaining to the website, its design and content, and all technical infrastructure relating to it. The trademarks and logos displayed on the website are MetFilm's registered and unregistered trademarks or those of others. You should not use any of the trademarks or other material on the website other than in accordance with this policy and any terms of use posted from time to time on the website.

12. Copyright

- 12.1. Use of the IT Systems to copy or transmit any documents, software or other information protected by copyright is prohibited unless the permission of the copyright owner has been obtained. Remember that copyright extends to video, music and images as well as text. In particular, before copying any material from the Internet read the copyright notice on the site and be sure to comply with it. Take care even where the website says you may freely copy any material made available on it, because sometimes copyright or other rights in such material does not in fact belong to the owner of the website or may be restricted to specific uses as such as personal use only or not for commercial use.

13. Contracts

- 13.1. You should be aware that if conducting dealings with external individuals, firms, companies, organisations or institutions, and other business contacts by e-mail, you could inadvertently create a binding contract on behalf of MetFilm with that external contact. You should only deal with external contacts by e-mail if you are employed and your job requires it. All figures should be typed both in words and numbers so as to avoid expensive clerical errors. Any business e-mails should be checked before despatch as carefully as you would check a written contract containing the same matters.

14. Security and Safeguarding the Network

- 14.1. You are responsible for the security of your laptop or computer terminal and must not allow your equipment to be used by any unauthorised person.
- 14.2. You should ensure any computer you use to access our IT Systems is protected with appropriate anti-virus software which is kept up to date.
- 14.3. If you have cause to be away from your workstation for any period you should log out or lock your equipment, otherwise we will be entitled to assume in the first instance that any material coming from or via your equipment was generated or passed on by you.
- 14.4. In addition to the account security you should ensure adequate physical security of any device left unattended.
- 14.5. The Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:
 - intentionally wasting staff effort or other MetFilm resources
 - corrupting, altering or destroying another User's data without their consent
 - disrupting the work of other Users or the correct functioning of the MetFilm Network
 - denying access to the MetFilm Network and its services to other users.
 - pursuance of commercial activities (excluding in support of MetFilm business). Contact IT Support to discuss your commercial need.
 - Any breach of industry good practice that is likely to damage the reputation of the JANET network will also be regarded as unacceptable use of the MetFilm Network.
 - Where the MetFilm Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the MetFilm Network.

14.6. Users shall not:

- introduce data-interception or network traffic logging, password-detecting or similar software or devices to MetFilm's Network;
- seek to gain unauthorized access to restricted areas of MetFilm's Network;
- access or try to access data where the user knows or ought to know that they should have no access;
- carry out any hacking activities
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

15. Software Use and Installation Restrictions

15.1. Software is subject to copyright and licensing restrictions. Software provided by MetFilm should only be used by members of MetFilm for academic, research and administrative purposes, and you should not copy or distribute it to others unless authorised to do so.

15.2. Do not install software onto MetFilm's IT systems without obtaining permission from the IT Department. You should not knowingly install software onto any of our IT systems (desktop systems and servers), without obtaining permission from the IT Department.

16. Monitoring and Processing of Data on IT Systems

16.1. Subject to the qualifications set out in this paragraph we will treat all messages sent, received or stored using the IT Systems as e-mails which relate to the operation, business or academic activities of MetFilm and neither staff nor students should have any expectation of privacy in any such messages.

16.2. We reserve the right to access, review, copy, process, delete or otherwise process any messages sent, received or stored on the IT Systems and to disclose any such messages (or information contained in them) to any person outside MetFilm where this is necessary for any purpose in connection with your employment or study in the following circumstances:

- to detect the unauthorised use of the IT Systems;
- to protect the IT Systems against viruses or hackers;
- to find lost messages or retrieve messages due to computer failure;
- to assist in the investigations of wrongful acts;
- to combat or investigate fraud or corruption;
- to prevent or detect crime;
- to comply with any legal obligation.
- to prevent the receipt of unsolicited communications that do not relate to the operation, business or academic activities of MetFilm.

16.3. We will take all reasonable steps to avoid opening or otherwise viewing the contents of e-mails which are marked "personal" in the subject heading unless we believe that such action is required in the circumstances set out in paragraph 8. E-mails marked "personal" will be subject to

traffic monitoring and automated interception to check for viruses in the same way as all other e-mails sent or received using the IT Systems.

16.4. We also reserve the right to monitor students' access to the Internet for any purpose in connection with engagement or study with MetFilm and in the following circumstances:

- to prevent or detect crime;
- to detect the unauthorised use of the Internet;
- to protect the IT Systems against viruses or hackers; or
- to combat or investigate fraud or corruption.

16.5. Where possible, monitoring of e-mail and Internet traffic will be limited to audits and monitoring traffic data unless routine monitoring or auditing justifies more detailed monitoring. However, we reserve the right to restrict access to individual or groups of a website should it be deemed appropriate to do so. Where possible automated monitoring will be used.

16.6. Information generated by monitoring Internet access and e-mail traffic will not normally be retained by us for more than one year. You are warned however that copies of all e-mails sent and received using the IT Systems can normally be retrieved after a significantly longer period, whether or not they are marked "personal".

17. Data protection

17.1. You should also refer to our Data Protection Policy which is available on our

https://www.metfilmschool.ac.uk/.../Policy_MetFilm_DataProtection_May2018_v2.3.pdf

You are reminded of the need to comply with the provisions of the Data Protection Act 2018, in particular with regard to the need to ensure the security and confidentiality of personal data (that is any information from which a living individual can be identified).

18. Leavers

18.1. On leaving MetFilm student e-mail accounts will be disabled/removed or downgraded to 'email only' status for alumni. Leavers will be provided with the date of this action.

Access to any other provided software (such as Adobe Creative Cloud) will also be removed.

18.2. In the event that it is deemed necessary to disable a user's e-mail account immediately, MetFilm reserve the right to action this without prior notice.

18.3. All leavers should therefore make all efforts to remove all documents before the account is closed. MetFilm cannot be held accountable for the loss of documents.

19. Discipline

19.1. Failure to adhere to this policy may result in disciplinary action. Please see the relevant student disciplinary procedures for more information.

19.2. Breaches of this policy which have serious or potentially serious adverse consequences for the operation, business or academic activities or reputation of MetFilm or the security and integrity of

the IT Systems and any breaches of section 8 of this policy may render a student in breach eligible for withdrawal from programme

20. Interpretation

20.1. This policy cannot cover every eventuality, particularly as the technology and its application is changing so rapidly. You are required to consider the purpose and objectives of this policy and to acknowledge that there are some uses of the Internet, e-mail facilities and related technology which, while not expressly forbidden by this policy, may still be regarded as inappropriate.

20.2. This policy will be reviewed and updated on a regular basis.

21. Equality Impact Assessment

22.1. The policy has been designed to ensure that all sections of our community can engage fully with our IT provision and have equal access to it.