Royal School of Needlework

RSN IT Policies — Version Summary

Control	
Version	1.0.2
Date	2020-02-17
Author	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Ownership:	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Approved by:	

Version History			
Version	**Changes**	**Author**	**Date**
1.0.2	Minor grammar and corrections to various policies; Approval by RSN Trustee Council	Scott Bartlett	2020-02-17
1.0.1	*Version number skipped*	n/a	n/a
1.0	Initial Version	Scott Bartlett	2020-01-31

Introduction

1. This document details the current versions of other RSN IT Policies and related documents
2. This document is updated from time to time and readers should proactively check for any updated version or changes.

Current Policy Versions

Version History			
Version	**Changes**	**Author**	**Date**
1.0.2	RSN Information Security Policy	Scott Bartlett	2020-02-17
1.0.2	RSN Data Protection Policy	Scott Bartlett	2020-02-17
1.0.2	RSN IT Usage Policy (Staff)	Scott Bartlett	2020-02-17
1.0.2	RSN IT Usage Policy (Students)	Scott Bartlett	2020-02-17
1.2.1	RSN Confidentiality Agreement (NDA)	Scott Bartlett	2020-02-17
Discontinued	RSN Social Media Policy *– now merged into IT Usage Policies*		

--- END OF DOCUMENT ---

Royal School of Needlework

RSN Data Protection Policy

Control	
Version	1.0.2
Date	2020-02-17
Author	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Ownership:	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Approved by:	RSN Trustees/Council

Version History			
Version	**Changes**	**Author**	**Date**
1.0.2	Fixed incorrect section numbering	Scott Bartlett	2020-02-17
1.0.1	Minor corrections for clarity ; correct numbering issue	Scott Bartlett	2020-01-30
1.0	Final	Scott Bartlett	2019-11-04
0.1-DRAFT	Initial draft.	Scott Bartlett	2019-10-14

Introduction

3. The Royal School of Needlework ('RSN') stores, processes and on occasion discloses information about employees, students and other Data Subjects for academic, administrative and commercial purposes.
4. The organisation recognises the need to comply with the laws and legislation regulating the processing of personal data. It is our aim that all RSN staff and other authorised data users recognise the risks involved when dealing with such information and fully understand the steps that must be taken in order to minimise such risks.
5. The organisation is committed to a policy of protecting the fundamental rights and freedoms of individuals and in particular their right to privacy with respect to the processing of personal data, as set out in:

   The Data Protection Act (2018), which includes the UK enactment of the EU's General Data Protection Regulation (2016/679) ('GDPR') plus updates to the Data Protection Act (1998).

   The Privacy in Electronic Communications (EC Directive) Regulations 2003, and all amendments.

Information processing

6. When handling such information, the RSN, and all staff or other authorised individuals or organisations who process or use any personal information will comply with the law in full at all times.
7. The organisation will utilise a 'privacy by design' and default approach to its collection and use of personal data and information which all staff must comply with.
8. The organisation will ensure that all processing of personal information carried out by the organisation is in accordance with data protection principles and legislation, in particular that:

   All personal information must be processed lawfully, fairly, and transparently;

   Personal information shall be obtained only for one or more specified and explicit lawful purpose(s) — i.e. 'purpose limitation';

   Personal information shall be adequate, relevant and necessary — i.e. 'data minimisation';

   Personal information shall be accurate and, where necessary, kept up to date;

Personal information shall not be retained for longer than is necessary for those purposes — i.e. ‘storage limitation’;

Personal information shall be processed in accordance with the rights of data subjects under the data protection legislation;

Appropriate security measures shall be taken against unauthorised or unlawful processing and against accidental loss or damage to or destruction of the information using appropriate technical or organisational measures — i.e. ‘integrity and confidentiality’;

Personal information shall not be transferred to a country outside the European Economic Area (‘EEA’) unless an adequate level of protection and supervision is in place.

9. Data protection legislation requires the organisation to process personal information fairly, lawfully and transparently. To this end this means that the organisation (including all staff, trustees, volunteers, tutors and other authorised parties) must comply with at least one of the following conditions when processing personal information:

    - The individual to whom the personal information relates has consented to the processing;
    - The processing is necessary for the performance of a contract between the RSN and the individual or another person or another party;
    - The processing is necessary in order to protect the vital interests of the individual;
    - The processing is necessary to comply with a legal obligation placed on the RSN;
    - The processing is necessary in order to pursue the legitimate interest of the data controller (i.e. the RSN) and is not unfair to the individual.

To ensure compliance with Data Protection law the RSN will:

10. Observe the spirit and the letter of the law and will not seek to exploit ambiguous wordings or "grey areas" to avoid its responsibilities.
11. Co-operate fully with the Information Commissioner and their office.
12. Establish procedures for day-to-day processing and storage of data. The procedures will provide a reference source for all staff to clarify anomalies, which may arise in routine operations.
13. Ensure that volunteers, contractors, suppliers and outsourced bodies who are processing personal data on the RSN’s behalf will be subject to Data Protection law, and necessary agreements will be in place.
14. Inform Data Subjects regarding the keeping of records, the processing of data and the disclosure of data to third parties, through the use of Privacy Notices.
15. Initiate and maintain an on-going programme of staff development with regard to data protection to educate and inform staff and other authorised data users about the dangers of inappropriate and illegal use of the personal data they may have access to.
16. Periodically review all policies and procedures to ensure continuing compliance with all relevant legislation.
17. Appoint a Data Protection Officer who will be responsible for advising staff of their obligations pursuant to data protection and for monitoring compliance with the legislation. The Data Protection Officer will also be responsible for external requests relating to data protection such as requests from any individual looking to exercise their rights under the data protection legislation.
18. Ensure that when individuals provide personal data to the RSN they are provided with a privacy notice to ensure the individual is advised who is gathering the information and how and for what purposes the organisation will process the provided information.

In order to minimise its liability in law the RSN will:

19. Ensure that all new data and information systems and new forms of processing data will be implemented in accordance with the legislation.

20. Conduct a privacy impact assessment on all necessary new projects, software or systems involving personal data.
21. Regard all members of staff (including tutors, volunteers and trustees and other authorised individuals or parties) of the RSN as having an obligation to divulge the existence and contents of databases or other soft or hard copy filing systems that contain personal data, to the Data Protection Officer or their nominee.
22. Implement and maintain appropriate practical and technical measures to ensure the security of all personal data.

Appendix A — Related Information Security policies

- IT Information Security Policy
- IT usage policy (Staff)
- IT usage policy (Students)
- *External:* UCA IT usage policy (Students) *(for RSN Degree Students)*

--- END OF DOCUMENT ---

Royal School of Needlework

RSN Information Security Policy

Control	
Version	1.0.2
Date	2020-02-17
Author	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Ownership:	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Approved by:	RSN Trustees/Council, 2020-02-17

Version History			
Version	**Changes**	**Author**	**Date**
1.0.2	Minor grammar and error corrections.	Scott Bartlett	2020-02-17
1.0.1	Minor fixes and corrections for clarity.	Scott Bartlett	2020-01-31
1.0	Final	Scott Bartlett	2019-11-08
0.2-DRAFT	Monitoring and Privacy updates	Scott Bartlett	2019-11-04
0.1-DRAFT	Initial restructuring draft.	Scott Bartlett	2019-10-14

Introduction

23. The Royal School of Needlework (RSN) recognises that information is a vital asset to any organisation and that information storage, sharing and systems play a critical role in supporting the organisation's strategic objectives.
24. The RSN recognises that information security is essential to the protection of the organisation's reputation and to the success of its academic, charity and administrative activities. In particular, the management of personal and financial data has important implications for individuals and is subject to legal obligations and the consequences of information security failures can be costly and time-consuming.
25. The RSN Information Security Policy is concerned with the management and use of the organisation's information assets and sets out appropriate measures through which the RSN will facilitate the secure and reliable flow of information, both within the RSN itself and in external communications. An information asset is defined as an item or body of information which is of value to the organisation.

Structure

26. The policy comprises this overarching document, which sets out the principles and framework, and a set of subordinate and specific policies, procedures and guidelines addressing individual aspects of security (see: *Appendix A*) which together constitute the Information Security Policy of the organisation. This approach is based on the recommendations contained in the University and Colleges Information Security Association's *UCISA Information Security Toolkit.* [https://www.ucisa.ac.uk].
27. Each of the sub-policy documents only contains high-level descriptions of requirements and principles. They do not, and are not intended to, include detailed descriptions of policy implementation. Such details will, where necessary, be provided in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents.

Purpose

28. The RSN Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets within the RSN in order to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which may otherwise occur.
29. The objective of the policy is to ensure that all information and information systems upon which the RSN depends are adequately protected to the appropriate level. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

Scope

30. The RSN Information Security Policy applies to information assets in all forms which are owned by the RSN or are used by the RSN with the approval of the relevant owner.
31. The information assets may be on paper, stored electronically or held on other media or material or in a non-electronic storage system.
32. The assets may include text, pictures, audio and video or a combination thereof.
33. The policy covers information delivered or transmitted by hand, post, by electronic means and by oral communication, including telephone and voicemail.
34. The policy applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.
35. The policy applies to all staff, trustees, tutors, volunteers, students and third-party contractors of the RSN.
36. The policy applies to the use of RSN owned systems and services as well as privately/externally owned systems when connected to the RSN network, systems or services directly or indirectly. (In this context, 'owned' is deemed to include leased, rented or on-loan including Internet cloud-based services).
37. The policy applies to all data and software owned or licensed to the RSN, be they loaded on RSN or privately/externally owned systems, and to all data and software provided to the RSN by donors, sponsors or external agencies.
38. The RSN *BA (Hons) Degree in Hand Embroidery* is validated by the *University for the Creative Arts* (UCA) and forms part of their portfolio of courses in the School of Craft and Design. UCA's own IT and information policies form part of this policy for RSN Degree students.

Responsibilities and Governance

Policy owners

39. Responsibility for the production, maintenance and communication of the policy lies with the RSN IT Manager who will promote awareness of and compliance with the policy, provide advice and guidance on good practice relating to the policy, and bring forward revisions to the policy as necessary. The IT Manager will report on a summary and exception basis, will notify issues and bring forward recommendations. Responsibility for maintaining the policy resides with the IT Manager.
40. The RSN Senior Management Team (SMT) is responsible for approving the Information Security policy (including any sub-policies) and for monitoring its implementation and for the actions required or remediations necessary from any identified breach or issue. This will be undertaken in consultation with the Trustees when identified as necessary.
41. The policy will be reviewed once a year and updated as needed to reflect changes to the RSN's objectives, needs, legal requirements and the risk environment.

Information owners

42. 'Owners' of information (such as customer, student or staff records) are responsible for defining the use of those assets and maintaining appropriate security measures.

43. An ‘Owner’ is normally deemed to be the Head of the Department which primarily owns and manages the business process utilising that information unless determined otherwise by the Senior Management Team (SMT) or IT Manager.

Systems administrators

44. The RSN IT manager is responsible for all electronic and digital RSN information systems and is responsible for ensuring that appropriate security arrangements are established, maintained and updated including ensuring vendor-supplied security patches are installed regularly as per relevant industry best practices.
45. The RSN IT manager is also responsible for carrying out periodic risk assessments of the security controls in place including taking into account changes in business requirements, changes in technology and any changes in the relevant legislation and must revise the security arrangements accordingly.
46. Access by contracted vendors of systems by remote access to enable maintenance and support will be granted only when required.

Information users

47. Information users are RSN staff, trustees, tutors, volunteers or other authorised parties who access or otherwise use the RSN’s information systems and information assets.
48. Heads of Departments and managers are responsible for ensuring that information and information systems used within their departments are managed and used in accordance with information security policies, protocols and guidelines. Heads of Departments are required to carry out periodic risk assessments and establish and maintain effective contingency plans.
49. Everyone granted access to RSN information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policies, codes of conduct and guidelines.
50. Each individual is responsible for protecting the RSN’s information assets, systems and infrastructure, and will at all times protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

Policy awareness and disciplinary procedures

51. This Information Security Policy will be made available to all staff, tutors, volunteers, trustees, authorised third parties and contractors (collectively ‘users’) requiring access to any RSN information systems and they will be advised of the existence of the relevant policies, codes of conduct and guidelines. Users will be asked to confirm that they understand the policy.
52. Changes or additions to the Policy may be proposed by any member of staff, via their Head of Department, to the IT Manager or Senior Management Team.
53. Failure to comply with the RSN Information Security Policy may lead to suspension or withdrawal of an individual’s access to information systems and services.
54. Failure to comply with the Information Security Policy may lead to the instigation of the relevant disciplinary procedures as specified in the RSN terms and conditions of employment and, in certain circumstances, legal action may be taken. Minor infringements, such as causing inconvenience to other users, may lead to a verbal or written warning. Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to a formal warning, suspension or termination of employment or termination of any formal or informal relationship with the RSN. This is not an exhaustive list of possible offences and the RSN will determine whether a case is minor or major having regard to all the circumstances of each incident.
55. Failure of a contractor or third-party to comply could lead to the cancellation of a contract and, in certain circumstances, legal action may be taken.

Policy Statement

56. The RSN is committed to protecting the security of information through the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure
- integrity: safeguarding the accuracy and completeness of information and processing methods
- availability: ensuring that information and associated services are available to authorised users when required

57. Information will be protected in line with all relevant policies and legislation, notably those relating to data protection, human rights and freedom of information.
58. Information will be made available only to those who have a legitimate need for access.
59. The RSN will develop, implement and maintain policies and procedures to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security.
60. Information will be protected against unauthorised access.
61. Compliance with the policy will be monitored and enforced.
62. In particular this policy will include but not be limited to the following policy requirements:

Authorised use

63. The RSN's information systems are provided to support the RSN's activities around its mission including teaching, research, administration, collection management and archiving, charity, donations and approved commercial business activities.
64. Only RSN staff and other persons or third parties authorised by the Senior Management Team or appropriate Head of Department are entitled to use the RSN's information systems. Such persons or parties may include but not be limited to trustees, tutors, volunteers, third-party contractors, strategic partners and students. Along with RSN staff these additional parties will be collectively referred to as 'users'.
65. It is the responsibility of all users who have been granted access to information to handle it appropriately in accordance with the policy.

Acceptable use

66. All users have an obligation to use information and information systems responsibly. Rules are defined in the *RSN IT Usage Policy (Staff)* and *RSN IT Usage Policy (Students)*.

Monitoring and privacy

67. The RSN respects the privacy of its users. Monitoring of user's Web and e-mail activity would constitute invasion of privacy unless it can be justified within a defined legitimate business purpose. The IT Department may keep records to monitor traffic flow and system usage but does not inspect the individual user data or content of e-mails unless the conditions of the *Regulation of Investigatory Powers Act* are met. Otherwise, the organisation performs no routine monitoring of e-mail content or individual Web access other than:

    To ensure the system's security and effective operation; e.g. to identify and stop possible viruses, malware or other electronic tools, methods, information or software which may be detrimental or dangerous to the safe and continued operation of the RSN's information systems or to the RSN's users or data; or to prevent access to websites or services which facilitate the distribution or operation of these tools.

    To identify and block websites or services which provide illegal or inappropriate content such as pornography, hate speech, illegal drugs and so forth. This may also include websites or services which themselves provide services or information which is either designed to or can be used to circumvent RSN IT security in order to access illegal or inappropriate content. What constitutes inappropriate content at any given time is the responsibility of the Senior Management Team in consultation with the IT Manager.

    To locate the storage or inclusion of payment card personal account numbers in transmitted data (which may include personal emails or documents) to ensure adherence to the *Payment Card Industry Data Security Standard*.

To establish the existence of facts relevant to the RSN: eg where there is a prima facie suspicion that the organisation's IT or telecommunications facilities have been misused or that the regulations governing the use of e-mail have been contravened.

To prevent or detect crime, including fraud or the infringement of IT related legislation such as the Computer Misuse Act 1990

68. The RSN reserves the right to make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers Act.
69. The RSN recognises that there may be instances where students may require legitimate access to potentially sensitive online material as part of their research activities. In such instances, academic approval is required prior to the completion of a registration for access from the IT Manager who will maintain a log. RSN Staff are similarly required to complete the registration for access.

Protection of software

70. All users must comply with the Copyright, Designs and Patents Act 1988 under which it is an offence to copy software or licensed products without the permission of the owner of the copyright.

Retention and disposal of information

71. All staff have a responsibility to consider security when using, storing and disposing of information in the course of their work. The RSN will determine retention periods for certain kinds of information and departments should establish procedures appropriate to the information held and processed by them and ensure that all users are aware of those procedures.

Virus and malware control

72. Users must not knowingly introduce, or take deliberate action to circumvent precautions taken to prevent the introduction of, a virus, malware, ransomware, worm, rootkit or any other kind of malicious or unapproved software item or service to any RSN owned system or service or the RSN network in general
73. If permitted to attach a personal device, such as a smartphone, tablet or laptop computer, to the RSN network or to an RSN system or service, users undertake to ensure the device is secured with appropriate, working and up-to-date anti-virus and antimalware software and to adhere to security best practices.

Business continuity

74. The RSN will implement, and regularly update, a business continuity management process to counteract interruptions to normal organisation activity and to protect critical processes and activities from the effects of failures or damage to vital services or facilities.

Information security education and training

75. The RSN recognises the need for all staff, tutors, volunteers and other users of RSN systems to be aware of information security threats and concerns, and to be equipped to support the organisation's security policy in the course of their normal work. Appropriate training or information on security matters will be provided for users and departments will supplement this to meet their particular requirements.

Breaches

76. All staff and other authorised users should report immediately any observed or suspected security incidents where a breach of the RSN's security policies has occurred, any security weaknesses in, or threats to, systems or services. Reports should be made to the Head of

Department or direct to the IT Manager or to any member of the Senior Management Team. The relevant Head of Department should investigate the report in conjunction with the IT Manager and, in the event that a weakness in or breach of security is found, this should be reported to the Senior Management Team.

Vulnerability testing

77. Regular internal and external vulnerability testing will be carried out by the IT department or an authorised third-party on a regular basis.

Legal and contractual requirements

78. The RSN will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing of information and, in particular, personal information. This includes but may not be limited to the following Acts for relevant parts or all of the operations of the RSN as applicable or required by law:

    Data Protection Act (2018) — which includes the UK enactment of the EU's GDPR (2016/679) regulation) plus updates to the Data Protection Act (1998)

    Protection of Freedoms Act (2012)

    Freedom of Information Act (2000)

    Regulation of Investigatory Powers Act (2000)

    Human Rights Act (1998)

    Computer Misuse Act 1990 including amendments in the Police and Justice Act (2006) and the Serious Crime Act (2015)

    Copyright Designs and Patents Act (1988) and applicable subsequent modifying regulations.

79. The RSN will also comply with all requirements related to the holding and processing of information in relation to:

    The terms and conditions of all licences, agreements and contracts

    Payment Card Industry Data Security Standard (PCI-DSS)

Appendix A — Related Information Security policies

- IT usage policy (Staff)
- IT usage policy (Students)
- *External:* UCA IT usage policy (Students)
- Data Protection policy

--- END OF DOCUMENT ---

Royal School of Needlework

RSN IT Usage Policy (Staff)

Control	
Version	1.0.2
Date	2020-02-17
Author	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Ownership:	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Approved by:	RSN Trustees/Council, 2020-02-17

Version History			
Version	**Changes**	**Author**	**Date**
1.0.2	Minor grammar and error corrections	Scott Bartlett	2020-02-17
1.0.1	Additional Prevent Duty text	Scott Bartlett	2020-01-24
1.0	Final	Scott Bartlett	2019-11-11
0.2-DRAFT	Merged social media policy	Scott Bartlett	2019-11-04
0.1-DRAFT	Initial restructuring draft including AUP	Scott Bartlett	2019-10-18

Introduction

1. The Royal School of Needlework (referred to hereafter as “the RSN”), promotes and facilitates the proper use of Information Technology in the interests of learning, research, creative practices, and business operations.
2. Because the RSN is ultimately responsible for the proper use of its IT facilities, it can therefore be held liable for any abuse of their use which breaches English or European Law, the policies of umbrella organisations, or breaches the contracts the RSN has with external partners or service providers.
3. This policy will refer to all computing tools, systems, services supplied or used, and electronic communications tools (including telephony), the associated physical environments, and any associated support as ‘RSN IT Resources’.
4. Guidelines and policies change from time to time; therefore, users are encouraged to ensure that they keep up-to-date and are familiar with this and other RSN policies which are available via their department head or the RSN IT department. If you have any query on this policy, please email your query to the RSN IT Manager – itmanager@royal-needlework.org.uk

Staff

5. For the purposes of this policy, ‘staff’ refers to:

   Full-time and part-time employees;

   Tutors;

   Volunteers;

   Board Trustees;

   Authorised contractors and third parties for a specific purpose or purposes;

6. The phrase ‘users’ is a generic phrase and in the context of this document and related documents refers to staff and other users of RSN IT resources in general.

Scope

7. This Policy applies to staff and other authorised users with respect of:

   using either personal or RSN provided equipment connected locally or remotely to the network of the RSN.

   all equipment connected (locally or remotely) to RSN IT Resources.

   the use of external networks and services that support the RSN's IT provision

   information that is recorded on, processed by, or output from RSN IT Resources

   the use of external online/cloud technologies such as wikis, blogs, discussion forums, social networks, collaboration technologies, file hosting services, data storage services and online office suites that are not part of the RSN IT services portfolio.

8. This Policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered. In the first instance staff should address questions concerning what is acceptable to their manager, Department Head or the IT Manager. Where there is any doubt the matter should be raised with a Departmental Head or the IT manager, who will ensure that all such questions are dealt with at the appropriate level within the RSN.
9. Wherever possible staff should use the RSN's official platforms and services. Users of externally hosted technologies must ensure that this use is approved by the IT Manager or Department head and that it is compliant with the law and the issues covered by this policy.

Core Principles

Overarching Legislation and Policies

10. All RSN staff members are subject to the policies and regulations of the RSN and to English and International law. The use of RSN IT Resources to create, store or distribute material that contravenes these regulations and laws can result in disciplinary or legal actions being taken against both the individuals responsible and the RSN as an organisation. The RSN has published specific policies on Information Security and Privacy which govern much of what is stated in this Policy and users should make themselves familiar with these policies particularly if their usage exposes them to personal or RSN sensitive information.

Liability

11. All users of RSN IT Resources are ultimately liable for what they produce and what they distribute through their use. The RSN may be equally culpable if it does not have in place policies and procedures to govern and police the proper usage of these facilities.

Interpretation

12. The laws that apply to the interpretation and impact of material created or distributed by one person to another are that it is the impact upon the recipient, intended or otherwise, rather than the intention of the creator or sender that applies in cases of harassment or offence.

Security

13. All IT systems and the files and media created through their use are valuable RSN assets that can be easily damaged or lost. It is the responsibility of all users to be aware of these risks and to use these facilities carefully and responsibly.

Acceptance of this Policy

14. The usage by staff of RSN IT Resources implies, and is conditional upon, acceptance of this Policy, for which a signature of acceptance may be required on joining the RSN.

15. The lack of a signature does not exempt an individual from any obligation under this Policy. It is the responsibility of all users of RSN IT Resources to read and understand this Policy.

Ownership and Intellectual Property Rights

16. Electronic communications documents pertaining to the business of the RSN are considered RSN documents whether or not the RSN owns the electronic communications facilities, systems or services used to create, store, or distribute them.
17. Electronic files that are created during academic and creative activities, such as, digital images, digital time-based media and creative writing remain the ownership of their authors.
18. All files created or edited by a staff member during the course of their duties, including electronic email files, are considered to be the property of the RSN.
19. Before using approved externally hosted services, users are responsible for consulting the service's terms and conditions to identify any IPR policy that may conflict with the RSN's policy.
20. Due to the risks of confidential information being released into the public domain inadvertently—e.g. information that may be commercially valuable—the use of cloud technologies must only be used with the prior written permission of a Departmental Head, the CEO or the IT Manager.

Publishing Externally

21. Due to reasons of ownership, data protection, intellectual property and copyright, the following content must not be made available on any part of the Internet not hosted by RSN or transmitted electronically without prior authorisation:

    Course handbooks

    Programme specifications

    Unit handbooks

    Essay and dissertation assignments

    Summative feedback or confidential feedback

    Formative assessment feedback

    Staff or student personal information

    Student or staff contact details

    RSN policies and procedures.

    Internal emails or other internal documents or items.

    Hampton Court Palace security and access policies and procedures.

    Any media for which you do not have permission to use

    Any material that could be considered defamatory, slanderous or libellous.

    Any other material that belongs to or is copyright to the organisation.

Freedom of Information

22. Users need to consider whether the use of an externally hosted service or technology will hinder compliance with the duties imposed on the RSN under the Freedom of Information Act (2000). The cloud is not an appropriate medium for sharing confidential information, and users are responsible for ensuring that information that is exempt from disclosure under the Freedom of Information Act is not posted onto an externally hosted service.

Data Protection

23. Users need to consider whether the use of an externally hosted service or technology will hinder compliance with the duties imposed on the RSN under the Data Protection Act (2018).
24. Users are responsible for ensuring that all personal information is processed in accordance with the RSN's Information Security policy.
25. The Cloud may not be an appropriate medium for sharing confidential information or personal data.

Counter Terrorism and Security Act 2015 and the Prevent Duty

26. Section 26 of the Counter Terrorism and Security Act places a duty on the RSN to have, in the exercise of its functions, due regard to the need to prevent staff and students being drawn into Terrorism. Under the guidance from HM Government, the RSN will maintain a record of network activity relating to access, attempted access, web traffic and threat analysis via remote analysis applications and shall take action where required. Data analysis of this nature is essential to ensure that the Security and Compliance of the RSN's IT infrastructure is maintained by preventing threats and violations including intrusion, unauthorised access, malicious code, licensing, pirating and copyright violations.
27. It is recognised that there may be instances where staff will need to access material which supports terrorism as part of their research activities. Staff who wish to access such material will need to receive approval from an academic member of staff and then register their need to access such material with the IT Manager and Departmental Head.
28. In the event that the RSN receives an internal or external enquiry regarding suspect security-sensitive material associated with the RSN or an RSN member, the RSN IT Department should be engaged to ensure that this matter is recorded and where necessary escalates this matter within the designated RSN's leadership team channels.

Purpose of Use

29. The RSN IT Resources are provided for the use of staff to support their work duties. The use of these facilities for personal use, such as personal electronic mail or recreational use of the Internet and World Wide Web is a privilege, not a right, that can be withdrawn. Any such use must not interfere with any other person's use of RSN IT Resources and must not, in any way, bring the RSN into disrepute.
30. The use of RSN IT Resources in support of non-RSN related activities requires explicit permission from the CEO. Such use, whether or not authorised, may be liable to charge.

RSN Domain Names, Trademarks and other Registered marks.

31. The RSN uses the registered names 'Royal School of Needlework' and 'RSN', and royal-needlework.org.uk as its principal internet domain names. All emails that originate from within any RSN domain will incorporate the RSN domain name in the email address, but this does not mean that the RSN automatically sanctions the content or views of all emails that originate or are forwarded from its domain.
32. 'RSN', 'Royal School of Needlework', 'royal-needlework.org.uk' or any other name, domain name, registration mark or trademark owned by or licenced to the RSN must not be used implicitly or explicitly in any way that suggests the RSN's endorsement of the content of an electronic data communication where this is not the case.

Authorisation

33. The RSN IT 'onboarding' procedure for a user grants authorisation to use the core IT facilities of the RSN. Following registration, a username and password will be allocated.
34. Authorisation to use other services may be granted automatically at the time of onboarding according to the user's needs or may be requested at a later date by applying to the IT Manager, Departmental Head or administrator, or the appropriate systems' administrator.

35. All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated.
36. Users are personally responsible and accountable for all activities carried out under their allocated username.
37. Attempts to access or use any account detail, username or password which is not authorised to the user, are prohibited and considered a serious breach of security and RSN policies.
38. Users must take all reasonable precautions to protect RSN resources and their personal account details, usernames, and passwords.

Passwords

39. The passwords used to log in to accounts and applications are subject to periodic change. Passwords, once expired, cannot be re-used.
40. Whenever a temporary password is allocated to facilitate a user's initial access to an account or application, this must be changed immediately following a successful login.
41. Passwords must not be disclosed to anyone even if the recipient is a member of IT Department support staff or authorised third-party or external support.
42. If you forget your password, contact a department administrator or the RSN IT Manager who will be able to help you.

Privacy

43. No member of RSN staff, including IT staff, will inspect individual user emails or content of personal files unless the conditions of overarching legislation in such areas is adhered to (see the RSN's Information Security Policy). However, there are times when the RSN is obliged to investigate the material it holds on its systems e.g:

    To ensure the system's security and effective operation; e.g. to identify and stop possible viruses, malware or other electronic tools, methods, information or software which may be detrimental or dangerous to the safe and continued operation of the RSN's information systems or to the RSN's users or data.

    To establish the existence of facts relevant to the RSN: e.g. where there is a prima facie suspicion that the organisation's IT facilities have been misused or that the policies and regulations governing the use of IT resources have been contravened.

    To or detect crime, including fraud or the infringement of IT related legislation such as the Computer Misuse Act 1990 upon receipt of a formal request from a law enforcement agency to release files that they require in pursuance of investigations that they may be carrying out.

    The RSN reserves the right to make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers Act.

44. Whilst the RSN sees privacy as desirable, it is not an absolute right, hence staff should not expect to hold or pass information, which they would not wish to be seen by authorised members of staff who may have privileged access to such areas to perform investigate duties.

Systems' Administration and Privacy

45. Systems administrators and authorised technical staff may be obliged to access any file, including electronic mail, stored on any system for which they have a responsibility to support. As the content of files cannot always be identified through their filename or location, this may necessitate opening multiple files until the required file or files are located.
46. Staff engaged in system support activities are bound by confidentiality clauses not to disclose any private information that they become privy to during the course of such activities.

Network Monitoring and Traffic Intercepts

47. Regular network monitoring is essential for ensuring that the RSN's IT systems function effectively, and any indication that there is a potential risk to its use may necessitate more focussed monitoring of specific network usage and high-volume users.
48. In some circumstances it may be necessary to intercept or stop network traffic in order to specifically identify the cause of performance issues or network bottlenecks. In such circumstances all reasonable steps will be taken to ensure the privacy of users.

Privacy to Others

49. When approaching or sitting near a user at a computer workstation or other device, what they may be working on may be private or RSN confidential and this privacy must be respected.
50. Where users share a printer, care must be taken when removing printed output that others printed matter is not retrieved and, if done so in error, the material must be passed to the owner if they are in the immediate vicinity or left at the printer for them to collect. Equally, if printing out confidential material using a shared printer, the printed output should be retrieved immediately.

Use of External Technologies

51. Users of these technologies must ensure that the RSN can still access the information and that the data is used, secured, managed and retired in line with any relevant RSN policies. Compliance with the FOI must always be considered in the use of these technologies.

Behaviour

General

52. No person shall perform any act that could jeopardise the integrity, performance or reliability of IT equipment, software, data and other stored information.
53. Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use, to make their use of it safe and effective and to avoid interference with the use of it by others.

Connection of Personal Devices to the Network

54. Although the RSN has in place systems for the prevention of damage caused by the distribution of malicious software (malware), such as computer virus programs, it is the responsibility of users to ensure that any personal device, for which *they* have responsibility and which is attached to the RSN network, is adequately protected through the use of up to date anti-virus software and has the latest tested security patches installed.

Harassment and Bullying

55. Distributing any material either physically or electronically which is deemed offensive, obscene or abusive, may not only be illegal but may also contravene RSN codes on harassment. Users of RSN IT Resources must familiarise themselves and comply with the RSN's code of conduct on harassment and bullying.

Equal Opportunities and Accessibility

56. The RSN is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.

Social Media

57. Social networks are web-based communication structures that enable easy communication and relationship building between individuals via the Internet, many of which include additional access to further methods of interaction, such as e-mail and instant messaging.
58. Whilst the RSN considers the widespread use of social networking applications an effective and useful method for communication in the appropriate context, the potential for misuse by staff and students, during and out of work hours, is such that the following guidelines are in place.
59. With specific regard to Social Media this policy has the following purpose:

    To help protect the organisation against potential liability;

    To give employees and other staff clear guidance on what can and cannot be said about the organisation or other students or staff;

    To help staff, tutors, academic staff and other authorised parties effectively manage the use of the organisation's resources;

    To help staff and students separate their professional and personal communication;

    To comply with the law on discrimination, data protection and protecting the health of employees;

    To be clear about the use of monitoring within the organisation.

60. The organisation will not tolerate staff using social networking sites for unofficial or inappropriate uses without proper authorisation and approval granted in advance. Specifically:

    You should not use such sites during contracted working hours for personal interest/benefit, without the authority of an appropriate manager. Usage during your agreed breaks is permitted, subject to the rules contained in this policy;

    You should not at any time express opinions which purport to be the opinion of the organisation, nor comments representing your own views on our organisation;

    You should not at any time upload photographs to your social networking sites of yourself or any other RSN staff member or student taken in an RSN work context, workplace or classroom situation;

    You should not at any time include information that identifies any other RSN staff member, tutor, volunteer, trustee, partner or any other individual working in connection with us;

    Any personal blogs should contain a disclaimer that the views expressed on it are personal views of the author only;

    You should not at any time make comments on such sites which bring the organisation into disrepute. No defamatory comments about the organisation should be made on such sites at any time.

    You should not at any time make comments on such sites which amount to bullying, harassment or any other detriment towards RSN staff member, tutor, volunteer, trustee, partner or any other individual working in connection with us;

61. The term "use" includes accessing social media by means of PC, mobile phone or by any other device or service or third-party.
62. It is highly recommended that all staff use strict privacy settings on their social network profiles.

Unacceptable Usage

Offensive, Obscene, or Indecent Material

63. Users must not create, propagate, or retain material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law, (see above).
64. The creation, dissemination, storage and display of indecent images of children is prohibited.

Processing Material that Supports Criminal or Terrorist Activities

65. Users must not create, propagate, or retain material that is associated with the support of terrorism or any other criminal activities.

Piracy and Intellectual Property Rights Infringement

66. Any activities which do not conform to UK and International law regarding the protection of intellectual property and data are prohibited. In accordance with the laws relating to Intellectual Property Rights, the downloading and copying of such files without the permission of the owner of the copyright is an illegal practice. The downloading, distribution, or storage of software, music, digital images, video and film clips, or other material for which you do not hold a valid licence, or other valid permission from the copyright holder, is not allowed.
67. Plagiarism, i.e. the intentional use of other people's material without attribution, is not allowed.

Abuse and Annoyance

68. Users must not use RSN IT Resources to harass, bully, or cause annoyance, inconvenience or needless anxiety to others. The creation, dissemination, storage and display of hate literature is prohibited.
69. The posting of defamatory comments about fellow staff or students on social networking sites is not allowed.

Defamation

70. Although genuine scholarly criticism is permitted, users must not create, propagate, or retain material that may be defamatory to another person, group, or organisation.

Email Misuse via Mass Emailing

71. The use of email for the distribution of emails to multiple addresses via email groups for frivolous or promotional purposes, aka ‘spamming’ is forbidden, as is the on forwarding of chain emails.

Fraudulent Use of System IDs

72. Engaging in any activities where a user accesses or uses systems under another user’s credentials is considered a major breach of security and may also be deemed fraudulent in law. Alleged misappropriation of another user’s ID or access rights may result in a temporary revocation of access to all RSN IT Resources for those users who may be implicated in the alleged breach while such allegations are investigated.
73. User must not send e-mails or post items on virtual learning environments or social networking sites that purport to come from an individual other than the person actually sending the message.

Malware

74. Users must be careful not to perform any actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software (aka malware).

Unauthorised System Activities

75. Users are not allowed to monitor or intercept network traffic. Users must not probe for the security weaknesses of systems.

76. Users are forbidden to attempt to break into or damage computer systems or data held thereon. Attempts to access, or actions intended to facilitate access, to computers for which the individual is not authorised is not allowed.
77. Users must not use the RSN network for unauthenticated access to any other system or service.
78. Staff must not connect unauthorised devices to the RSN network, without prior consultation with IT Services, except via the RSN's approved wifi connectivity services.

Commercial Activities

79. Commercial use of the RSN's internet access contravenes the acceptable use policy and is not permissible. The use of RSN IT Resources must not be used in support of external voluntary or charitable activities unless express permission has been granted; there may be a charge for such usage.
80. The use of RSN business mailing lists without proper authorisation is forbidden.
81. The conduct of e-mail correspondence which could lead to the inadvertent formation of a contract binding upon the RSN must not be undertaken.
82. Users are not allowed to resell RSN services or information.
83. RSN IT Resources must not be offered for use to individual consumers or organisations outside the RSN except where such services support the mission of the RSN or are in the commercial interest of the RSN and have been granted permission by a head of Department, the CEO or the IT Manager.

Frivolous Use

84. Non-work activities which generate heavy network traffic or interfere with others' legitimate use of RSN IT Resources are not allowed. This may include but not be limited to: personal large file transfers; system updates or online backup for personal devices; video or audio streaming.

Loss and Damage

85. Save as set out below, the RSN (including its affiliates, officers, agents and employees) accepts no liability to users for:

    the malfunctioning of any IT facility or part thereof, whether hardware, software or other.

    any loss or damage incurred by a user as a result of personal use of RSN IT Resources. Users should not rely on personal use of RSN electronic communications facilities for communications that might be sensitive with regard to timing, financial effect, privacy or confidentiality.

    for the acts or omissions of other providers of telecommunications services or for faults in or failures of their networks and equipment.

    for the loss of data in the cloud.

86. The RSN does not exclude its liability under this Policy to users:

    for personal injury or death resulting from the RSN's negligence.

    for any matter which it would be illegal for the RSN to exclude or to attempt to exclude its liability.

    for fraudulent misrepresentation.

87. Users agree not to cause any form of damage to the RSN's IT facilities, or to any accommodation or service associated with them. Should such damage arise the RSN shall be entitled to recover from such user, by way of indemnity, any and all losses, costs, damages and/or expenses that the RSN incurs or suffers as a result of such damage.

Health and Safety

88. The RSN strives to ensure that its facilities are used sensibly and responsibility and has a wide range of policies in these areas.

Deletion of Data

89. Users should be aware that data deleted from computer disks by the user may still be accessible in some cases via certain system tools.
90. Once sent outside the jurisdiction of the RSN, the withdrawal or deletion of data may not be possible.

Back-up Services

91. The RSN performs regular daily backups of core IT systems and resources.
92. The daily back-up process may result in the copying of data to either storage media or cloud services that might be retained for periods of time in locations unknown to the originator or recipient of electronic communications.
93. The practice and frequency of back-ups and the retention of back-up copies vary from system to system and may be changed or updated at any time by the IT Manager as seen fit.
94. Data can sometimes be susceptible to corruption due to hardware or software failure. IT staff would make reasonable attempts to recover data however it might not be possible to do this in all situations.

Software and Hardware Auditing

95. The RSN has an obligation to ensure that only legal software is used on RSN owned equipment and to support this, appropriate technology may be used to audit all software that has been installed on RSN owned equipment without appropriate permission.
96. The Board of Trustees, CEO, Heads of Department and the IT Manager may be notified of any illegal software discovered as part of the audit process.

Removal of Equipment

97. No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location, without the explicit permission of the IT Manager, or other appropriately authorised member of staff.
98. No equipment can be taken out of the RSN premises without the explicit permission of the appropriate department head or the IT Manager. For permission to be granted the necessary forms detailing the purpose of the removal of the equipment and the equipment details must be filled by the applicant and countersigned by the appropriate manager or owner as mentioned above.

Telephone Systems

99. The law protects the privacy of telephone conversations. Without court approval, it is illegal to record or monitor audio or visual telephone conversations without advising the participants in advance that the call is being monitored or recorded.
100. The use of RSN telephone equipment creates transaction records (which include the number called and the time and length of the call) that are reviewed by the RSN Senior Management Team and Departmental Heads as part of routine accounting procedures.

Investigation and Response to IT violations

Policy

101. Instances of breaches may be drawn to the attention of the IT Manager and Senior Management Team via internal or external complaints, the intrusion detection system, or discovered in the normal course of business.
102. The actions taken because of a policy violation are dependent on the particular circumstances.

Immediate Response

103. The IT Manager will the impact of the alleged violation and take, without notice, any necessary action if RSN resources and services are adversely affected to prevent immediate and further damage to the RSN network. Such actions may include:

    Suspension of an account

    Disconnection of systems or disable network ports

    Termination of running processes and programs

    Any other actions deemed necessary to restore network services.

Investigation of Alleged Violations

104. The IT Manager (with assistance if required) will gather evidence and provide information as directed by the Senior Management Team or appropriate Heads of Departments to comply with any internal investigation. In some cases, the users may not be notified first or it may be required by law to provide the information without notifying the user. Investigations into complaints may necessitate the examination of systems and network activity logs and transaction logs. Contents of emails and other files will not be examined as part of a routine except in the following circumstances without the holder being notified:

    A court order requires that the content be examined and disclosed.

    The IT Manager is instructed in writing either by the CEO or Finance Director or Operations Manager or Board of Trustees as part of an internal investigation.

105. If the violation does not prevent other users from accessing network computer resources or result in a disciplinary procedure being instigated, the matter will be referred to the appropriate administrative authority for disciplinary action if the user refuses to comply.

Reporting Security Incidents

106. All users of RSN IT Resources are encouraged to note and report any observed or suspected security incidents, security weaknesses in or threats to systems and services. Such reports can be made at the local campus helpdesks.

Disciplinary Action

107. Users whose actions contravene the guidelines within the RSN IT Policy or any of its related policies will find themselves subject to disciplinary proceedings as defined within their employment contract or other applicable contract with the RSN.
108. Individuals in contravention of the RSN IT policy may also be subject to criminal proceedings. The RSN reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this Policy.

--- END OF DOCUMENT

Royal School of Needlework

RSN IT Usage Policy (Students)

Control	
Version	1.0.2
Date	2020-02-17
Author	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Ownership:	Scott Bartlett, IT Manager (scott.bartlett@royal-needlework.org.uk)
Approved by:	RSN Trustees/Council, 2020-02-17

Version History			
Version	**Changes**	**Author**	**Date**
1.0.2	Minor grammar and error corrections	Scott Bartlett	2020-02-17
1.0.1	*Version number skipped*	n/a	n/a
1.0	Final	Scott Bartlett	2019-11-11
0.2-DRAFT	Merged social media policy	Scott Bartlett	2019-11-04
0.1-DRAFT	Initial restructuring draft including AUP	Scott Bartlett	2019-10-18

Introduction

1. The Royal School of Needlework (referred to hereafter as “the RSN”), promotes and facilitates the proper use of Information Technology in the interests of learning, research, creative practices, and business operations.
2. Because the RSN is ultimately responsible for the proper use of its IT facilities, it can therefore be held liable for any abuse of their use which breaches English or European Law, the policies of umbrella organisations, or breaches the contracts the RSN has with external partners or service providers.
3. This policy will refer to all computing tools, systems, services supplied or used, and electronic communications tools (including telephony), the associated physical environments, and any associated support as ‘RSN IT Resources’.
4. Guidelines and policies change from time to time; therefore, users are encouraged to ensure that they keep up-to-date and are familiar with this and other RSN policies which are available via their department head or the RSN IT department. If you have any query on this policy, please email your query to the RSN IT Manager – itmanager@royal-needlework.org.uk

Students

5. The RSN provides educational courses and classes in a number of formats, including:

   Day Classes,

   Certificate and Diploma courses (‘c&d’)

   BA (Hons) Degree in Hand Embroidery (‘degree’)

   Future Tutors (‘FT’) course.

6. Only students on the degree and FT courses are granted required access to RSN IT facilities via a personal, unique login identity and are subject to this policy.
7. Students attending Day Classes or C&D Classes are *not* granted access to any RSN IT facilities apart from secure ‘guest wifi’ in the classroom areas.
8. *For the purposes of the rest of this policy, ‘students’ refers to degree and FT students who have a personal, unique login identity for the RSN network.*

Degree Students

9. The RSN BA (Hons) Degree in Hand Embroidery is verified by the University of the Creative Arts ('UCA') and all students on this course ('degree') are enrolled as UCA students.
10. All RSN degree course students are subject to UCA's own policies in addition to this policy with regard to IT facilities and usage, and those relevant UCA policies should be read and followed in conjunction with this policy.

Scope

11. This Policy applies to students with respect of:

    using either personal or RSN provided equipment connected locally or remotely to the network of the RSN.

    all equipment connected (locally or remotely) to RSN IT Resources.

    the use of external networks and services that support the RSN's IT provision

    information that is recorded on, processed by, or output from RSN IT Resources

    the use of external online/cloud technologies such as wikis, blogs, discussion forums, social networks, collaboration technologies, file hosting services, data storage services and online office suites that are not part of the RSN IT services portfolio.

12. This Policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered. In the first instance students should address questions concerning what is acceptable to their course tutor. Where there is any doubt the matter should be raised with a Departmental Head or the IT manager, who will ensure that all such questions are dealt with at the appropriate level within the RSN.
13. The RSN wishes to encourage the use of appropriate cloud technologies and services, and wherever possible staff and students should use the RSN's official platforms and services. Users of externally hosted technologies must ensure that this use is compliant with the law and the issues covered by this policy.

Core Principles

Overarching Legislation and Policies

14. All members of the RSN are subject to the policies and regulations of the RSN and to English and International law. The use of RSN IT Resources to create, store or distribute material that contravenes these regulations and laws can result in disciplinary or legal actions being taken against both the individuals responsible and the RSN as an organisation. The RSN has published specific policies on Information Security and Privacy which govern much of what is stated in this Policy and users should make themselves familiar with these policies particularly if their usage exposes them to personal or RSN sensitive information.

Liability

15. All users of RSN IT Resources are ultimately liable for what they produce and what they distribute through their use. The RSN may be equally culpable if it does not have in place policies and procedures to govern and police the proper usage of these facilities.

Interpretation

16. The laws that apply to the interpretation and impact of material created or distributed by one person to another are that it is the impact upon the recipient, intended or otherwise, rather than the intention of the creator or sender that applies in cases of harassment or offence.

Security

17. All IT systems and the files and media created through their use are valuable RSN assets that can be easily damaged or lost. It is the responsibility of all users to be aware of these risks and to use these facilities carefully and responsibly.

Acceptance of this Policy

18. The registration of a student to use, or the actual usage by a student of, RSN IT Resources implies, and is conditional upon, acceptance of this Policy, for which a signature of acceptance may be required on joining the RSN or relevant RSN course.
19. The lack of a signature does not exempt an individual from any obligation under this Policy. It is the responsibility of all users of RSN IT Resources to read and understand this Policy.

Ownership and Intellectual Property Rights

20. Electronic communications documents pertaining to the business of the RSN are considered RSN documents whether or not the RSN owns the electronic communications facilities, systems or services used to create, store, or distribute them.
21. Electronic files that are created during academic and creative activities, such as, digital images, digital time-based media and creative writing remain the ownership of their authors.
22. When a student leaves the RSN, files which are left behind on any computer system owned by the RSN, including electronic email files, will be considered to be the property of the RSN. It is up to the leaver to ensure that they have cleared their electronic folders of private material.
23. Before using externally hosted services, users are responsible for consulting the service's terms and conditions to identify any IPR policy that may conflict with the RSN's policy.
24. Due to the risks of confidential information being released into the public domain inadvertently—e.g. information that may be commercially valuable—the use of cloud technologies must only be used with the prior written permission of a Departmental Head, the CEO or the IT Manager.

Publishing Externally

25. Due to reasons of ownership, data protection, intellectual property and copyright, the following content must not be made available on any part of the Internet not hosted by RSN or transmitted electronically without prior authorisation:

    Course handbooks

    Programme specifications

    Unit handbooks

    Essay and dissertation assignments

    Summative feedback or confidential feedback

    Formative assessment feedback

    Staff or student personal information

    Student or staff contact details

    RSN policies and procedures.

    Hampton Court Palace security and access policies and procedures.

    Any media for which you do not have permission to use

    Any material that could be considered defamatory, slanderous or libellous.

Freedom of Information

26. Users need to consider whether the use of an externally hosted service or technology will hinder compliance with the duties imposed on the RSN under the Freedom of Information Act (2000). The cloud is not an appropriate medium for sharing confidential information, and users are responsible for ensuring that information that is exempt from disclosure under the Freedom of Information Act is not posted onto an externally hosted service.

Data Protection

27. Users need to consider whether the use of an externally hosted service or technology will hinder compliance with the duties imposed on the RSN under the Data Protection Act (2018).
28. Users are responsible for ensuring that all personal information is processed in accordance with the RSN's Information Security policy.
29. The Cloud may not be an appropriate medium for sharing confidential information or personal data.

Counter Terrorism and Security Act 2015 and the Prevent Duty

30. Section 26 of the Counter Terrorism and Security Act places a duty on the RSN to have, in the exercise of its functions, due regard to the need to prevent staff and students being drawn into Terrorism. Under the guidance from HM Government, the RSN will maintain a record of network activity relating to access, attempted access, web traffic and threat analysis via remote analysis applications and shall take action where required. Data analysis of this nature is essential to ensure that the Security and Compliance of the RSN's IT infrastructure is maintained by preventing threats and violations including intrusion, unauthorised access, malicious code, licensing, pirating and copyright violations.
31. It is recognised that there may be instances where students will need to access material which supports terrorism as part of their research activities. Students who wish to access such material will need to receive approval from an academic member of staff and then register their need to access such material with the IT Manager and Departmental Head.
32. In the event that the RSN receives an internal or external enquiry regarding suspect security-sensitive material associated with the RSN or an RSN member, the RSN IT Department should be engaged to ensure that this matter is recorded and where necessary escalates this matter within the designated RSN's leadership team channels.

Purpose of Use

33. The RSN IT Resources are provided for the use of students to support their academic and creative endeavours. The use of these facilities for personal use, such as personal electronic mail or recreational use of the Internet and World Wide Web is a privilege, not a right, that can be withdrawn. Any such use must not interfere with any other person's use of RSN IT Resources and must not, in any way, bring the RSN into disrepute.
34. The use of RSN IT Resources in support of non-RSN related activities requires explicit permission from the CEO. Such use, whether or not authorised, may be liable to charge.

RSN Domain Names, Trademarks and other Registered marks.

35. The RSN uses the registered names 'Royal School of Needlework' and 'RSN', and royal-needlework.org.uk as its principal internet domain names. All emails that originate from within an RSN domain will incorporate the RSN domain name in the email address, but this does not mean that the RSN automatically sanctions the content or views of all emails that originate or are forwarded from its domain.
36. 'RSN', 'Royal School of Needlework', 'royal-needlework.org.uk' or any other name, domain name, registration mark or trademark owned by or licenced to the RSN must not be used implicitly or explicitly in any way that suggests the RSN's endorsement of the content of an electronic data communication where this is not the case.

Authorisation

37. The RSN IT 'onboarding' procedure for a student grants authorisation to use the core IT facilities of the RSN. Following registration, a username and password will be allocated.
38. Authorisation to use other services may be granted automatically at the time of onboarding according to the user's needs or may be requested at a later date by applying to the IT Manager, Departmental Head or administrator, or the appropriate systems' administrator.
39. All individually allocated usernames, passwords and electronic certificates are for the exclusive use of the individual to whom they are allocated.
40. Users are personally responsible and accountable for all activities carried out under their allocated username.
41. Attempts to access or use any account detail, username or password which is not authorised to the user, are prohibited and considered a serious breach of security and RSN policies.
42. Users must take all reasonable precautions to protect RSN resources and their personal account details, usernames, and passwords.

Email

43. The RSN does not, as standard, provide an email service to students. RSN email services are restricted to RSN staff and authorised volunteers.
44. Degree students should use their UCA-provided email address for all RSN email purposes and communications.
45. For all other students, any used email service is a personal choice and matter but usage for RSN purposes or communications must abide by this policy, in particular with regard to security and confidentiality.

Passwords

46. The passwords used to log in to accounts and applications are subject to periodic change. Passwords, once expired, cannot be re-used.
47. Whenever a temporary password is allocated to facilitate a user's initial access to an account or application, this must be changed immediately following a successful login.
48. Passwords must not be disclosed to anyone even if the recipient is a member of IT Department support staff or authorised third-party or external support.
49. If you forget your password, contact a department administrator or the RSN IT Manager who will be able to help you.

Privacy

50. No member of RSN staff, including IT staff, will inspect individual user emails or content of personal files unless the conditions of overarching legislation in such areas is adhered to (see the RSN's Information Security Policy). However, there are times when the RSN is obliged to investigate the material it holds on its systems e.g:

    To ensure the system's security and effective operation; e.g. to identify and stop possible viruses, malware or other electronic tools, methods, information or software which may be detrimental or dangerous to the safe and continued operation of the RSN's information systems or to the RSN's users or data.

    To establish the existence of facts relevant to the RSN: e.g. where there is a prima facie suspicion that the organisation's IT facilities have been misused or that the policies and regulations governing the use of IT resources have been contravened.

    To prevent or detect crime, including fraud or the infringement of IT related legislation such as the Computer Misuse Act 1990 upon receipt of a formal request from a law enforcement agency to release files that they require in pursuance of investigations that they may be carrying out.

The RSN reserves the right to make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers Act.

51. Whilst the RSN sees privacy as desirable, it is not an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by authorised members of staff who may have privileged access to such areas to perform investigate duties.

Systems' Administration and Privacy

52. Systems administrators and authorised technical staff may be obliged to access any file, including electronic mail, stored on any system for which they have a responsibility to support. As the content of files cannot always be identified through their filename or location, this may necessitate opening multiple files until the required file or files are located.
53. Staff engaged in system support activities are bound by confidentiality clauses not to disclose any private information that they become privy to during the course of such activities.

Network Monitoring and Traffic Intercepts

54. Regular network monitoring is essential for ensuring that the RSN's IT systems function effectively, and any indication that there is a potential risk to its use may necessitate more focussed monitoring of specific network usage and high-volume users.
55. In some circumstances it may be necessary to intercept or stop network traffic in order to specifically identify the cause of performance issues or network bottlenecks. In such circumstances all reasonable steps will be taken to ensure the privacy of users.
56. The RSN currently content filters web traffic (by URL domain) from the Internet in order to identify and block traffic from malicious sources (e.g. identified or potential malware and botnet sites) and from certain types of website based on categorisation (e.g. pornography, violence/hate/racism, weapons, illegal drugs, etc.). The RSN recognises that there may be instances where students may require legitimate access to potentially sensitive online material as part of their research activities. In such instances, academic approval is required prior to the completion of a registration for access from the IT Manager who will maintain a log. RSN Staff are similarly required to complete the registration for access.

Privacy to Others

57. When approaching or sitting near a user at a computer workstation or other device, what they may be working on may be private or RSN confidential and this privacy must be respected.
58. Where users share a printer, care must be taken when removing printed output that others printed matter is not retrieved and, if done so in error, the material must be passed to the owner if they are in the immediate vicinity or left at the printer for them to collect. Equally, if printing out confidential material using a shared printer, the printed output should be retrieved immediately.

Use of External Technologies

59. Users of these technologies must ensure that the RSN can still access the information and that the data is used, secured, managed and retired in line with any relevant RSN policies. Compliance with the FOI must always be considered in the use of these technologies.

Behaviour

General

60. No person shall perform any act that could jeopardise the integrity, performance or reliability of IT equipment, software, data and other stored information.

61. Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use, to make their use of it safe and effective and to avoid interference with the use of it by others.

Connection of Personal Devices to the Network

62. Although the RSN has in place systems for the prevention of damage caused by the distribution of malicious software (malware), such as computer virus programs, it is the responsibility of users to ensure that any personal device, for which *they* have responsibility and which is attached to the RSN network, is adequately protected through the use of up to date anti-virus software and has the latest tested security patches installed.

Use of Plug-in Speakers and Headphones

63. Plug-in speakers must not be used with RSN IT equipment in shared environments such as the IT Suite, Degree Library or shared classroom or office space.
64. Headphones may be used but only at a volume where there is no sound leakage that could disturb other users.
65. If inconsiderate use of headphones causes a nuisance to other users, such users have a right to ask for the volume to be reduced or else register a complaint with the appropriate department head or administrator responsible for managing the shared space in question.

Harassment and Bullying

66. Distributing any material either physically or electronically which is deemed offensive, obscene or abusive, may not only be illegal but may also contravene RSN codes on harassment. Users of RSN IT Resources must familiarise themselves and comply with the RSN's code of conduct on harassment and bullying.

Equal Opportunities and Accessibility

67. The RSN is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.

Social Media

68. Social networks are web-based communication structures that enable easy communication and relationship building between individuals via the Internet, many of which include additional access to further methods of interaction, such as e-mail and instant messaging.
69. Whilst the RSN considers the widespread use of social networking applications an effective and useful method for communication in the appropriate context, the potential for misuse by staff and students, during and out of work hours, is such that the following guidelines are in place.
70. With specific regard to Social Media this policy has the following purpose:

    To help protect the organisation against potential liability;

    To give students clear guidance on what can and cannot be said about the organisation or other students or staff;

    To help tutors, academic staff and other authorised staff effectively manage the use of the organisation's resources;

    To help students separate their professional and personal communication;

    To comply with the law on discrimination, data protection and protecting the health of employees;

    To be clear about the use of monitoring within the organisation.

71. The organisation will not tolerate students using social networking sites for unofficial or inappropriate uses without proper authorisation and approval granted in advance. Specifically:

    You should not at any time express opinions which purport to be the opinion of the organisation, nor comments representing your own views on our organisation;

    You should not at any time upload photographs to your social networking sites of yourself or any other student or RSN staff member taken in an RSN context or classroom situation;

    You should not at any time include information that identifies any other RSN staff member, tutor, volunteer, trustee, partner or any other individual working in connection with us;

    Any personal blogs should contain a disclaimer that the views expressed on it are personal views of the author only;

    You should not at any time make comments on such sites which bring the organisation into disrepute. No defamatory comments about the organisation should be made on such sites at any time.

    You should not at any time make comments on such sites which amount to bullying, harassment or any other detriment towards RSN staff member, tutor, volunteer, trustee, partner or any other individual working in connection with us;

72. The term “use” includes accessing social media by means of PC, mobile phone or by any other device or service or third-party.
73. It is highly recommended that all students use strict privacy settings on their social network profiles.

Unacceptable Usage

Creative Practice vs Moral and Social Sensitivities

74. Conventional norms of behaviour apply to IT-based media, just as they would apply to more traditional media, but a policy such as this cannot anticipate all the issues that might arise in the use of IT facilities in pursuance of academic or creative activities, particularly those that border the boundaries of sensitivity regarding religious or moral values.
75. Where academic endeavours appear to confront such areas, students must liaise with their tutors to ensure that the study or practise is executed whilst recognising the intertwining legal, institutional, individual, and creative interests involved. Within the RSN setting this should be taken to mean that the tradition of academic and creative freedoms will always be respected and where the integrity of such endeavours can be clearly argued for or demonstrated, the RSN will seek to support this in a managed way.

Offensive, Obscene, or Indecent Material

76. Users must not create, propagate, or retain material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law, (see above).
77. The creation, dissemination, storage and display of indecent images of children is prohibited.

Processing Material that Supports Criminal or Terrorist Activities

78. Users must not create, propagate, or retain material that is associated with the support of terrorism or any other criminal activities.

Piracy and Intellectual Property Rights Infringement

79. Any activities which do not conform to UK and International law regarding the protection of intellectual property and data are prohibited. In accordance with the laws relating to Intellectual Property Rights, the downloading and copying of such files without the permission

of the owner of the copyright is an illegal practice. The downloading, distribution, or storage of software, music, digital images, video and film clips, or other material for which you do not hold a valid licence, or other valid permission from the copyright holder, is not allowed.

80. Plagiarism, i.e. the intentional use of other people's material without attribution, is not allowed.

Abuse and Annoyance

81. Users must not use RSN IT Resources to harass, bully, or cause annoyance, inconvenience or needless anxiety to others. The creation, dissemination, storage and display of hate literature is prohibited.
82. The posting of defamatory comments about staff or fellow students on social networking sites is not allowed.

Defamation

83. Although genuine scholarly criticism is permitted, users must not create, propagate, or retain material that may be defamatory to another person, group, or organisation.

Email Misuse via Mass Emailing

84. The use of email for the distribution of emails to multiple addresses via email groups for frivolous or promotional purposes, aka ‘spamming’ is forbidden, as is the on forwarding of chain emails.

Fraudulent Use of System IDs

85. Engaging in any activities where a user accesses or uses systems under another user’s credentials is considered a major breach of security and may also be deemed fraudulent in law. Alleged misappropriation of another user’s ID or access rights may result in a temporary revocation of access to all RSN IT Resources for those users who may be implicated in the alleged breach while such allegations are investigated.
86. User must not send e-mails or post items on virtual learning environments or social networking sites that purport to come from an individual other than the person actually sending the message.

Malware

87. Users must be careful not to perform any actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software (aka malware).

Unauthorised System Activities

88. Students are not allowed to monitor or intercept network traffic. Students must not probe for the security weaknesses of systems.
89. Users are forbidden to attempt to break into or damage computer systems or data held thereon. Attempts to access, or actions intended to facilitate access, to computers for which the individual is not authorised is not allowed.
90. Users must not use the RSN network for unauthenticated access to any other system or service.
91. Students must not connect unauthorised devices to the RSN network, without prior consultation with IT Services, except via the RSN’s approved wifi connectivity services.

Commercial Activities

92. Commercial use of the RSN’s internet access contravenes the acceptable use policy and is not permissible. The use of RSN IT Resources must not be used in support of external

voluntary or charitable activities unless express permission has been granted; there may be a charge for such usage.

93. The use of RSN business mailing lists without proper authorisation is forbidden.
94. The conduct of e-mail correspondence which could lead to the inadvertent formation of a contract binding upon the RSN must not be undertaken.
95. Users are not allowed to resell RSN services or information.
96. RSN IT Resources must not be offered for use to individual consumers or organisations outside the RSN except where such services support the mission of the RSN or are in the commercial interest of the RSN and have been granted permission by a head of Department, the CEO or the IT Manager.

Frivolous Use

97. Non-academic activities which generate heavy network traffic or interfere with others' legitimate use of RSN IT Resources are not allowed. This may include but not be limited to: personal large file transfers; system updates or online backup for personal devices; video or audio streaming.

Loss and Damage

98. Save as set out below, the RSN (including its affiliates, officers, agents and employees) accepts no liability to users for:

    the malfunctioning of any IT facility or part thereof, whether hardware, software or other.

    any loss or damage incurred by a user as a result of personal use of RSN IT Resources. Users should not rely on personal use of RSN electronic communications facilities for communications that might be sensitive with regard to timing, financial effect, privacy or confidentiality.

    for the acts or omissions of other providers of telecommunications services or for faults in or failures of their networks and equipment.

    for the loss of data in the cloud.

99. The RSN does not exclude its liability under this Policy to users:

    for personal injury or death resulting from the RSN's negligence.

    for any matter which it would be illegal for the RSN to exclude or to attempt to exclude its liability.

    for fraudulent misrepresentation.

100. Users agree not to cause any form of damage to the RSN's IT facilities, or to any accommodation or service associated with them. Should such damage arise the RSN shall be entitled to recover from such user, by way of indemnity, any and all losses, costs, damages and/or expenses that the RSN incurs or suffers as a result of such damage.

Health and Safety

101. The RSN strives to ensure that its facilities are used sensibly and responsibility and has a wide range of policies in these areas.

Deletion of Data

102. Users should be aware that data deleted from computer disks by the user may still be accessible in some cases via certain system tools.
103. Once sent outside the jurisdiction of the RSN, the withdrawal or deletion of data may not be possible.

Back-up Services

104. The RSN performs regular daily backups of core IT systems and resources.
105. The daily back-up process may result in the copying of data to either storage media or cloud services that might be retained for periods of time in locations unknown to the originator or recipient of electronic communications.
106. The practice and frequency of back-ups and the retention of back-up copies vary from system to system and may be changed or updated at any time by the IT Manager as seen fit.
107. Data can sometimes be susceptible to corruption due to hardware or software failure and users are encouraged to keep backups of their own data. IT staff would make reasonable attempts to recover data however it might not be possible to do this in all situations.

Software and Hardware Auditing

108. The RSN has an obligation to ensure that only legal software is used on RSN owned equipment and to support this, appropriate technology may be used to audit all software that has been installed on RSN owned equipment without appropriate permission.
109. The Board of Trustees, CEO, Heads of Department and the IT Manager may be notified of any illegal software discovered as part of the audit process.

Removal of Equipment

110. No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location, without the explicit permission of the IT Manager, or other appropriately authorised member of staff.
111. No equipment can be taken out of the RSN premises without the explicit permission of the appropriate department head or the IT Manager. For permission to be granted the necessary forms detailing the purpose of the removal of the equipment and the equipment details must be filled by the applicant and countersigned by the appropriate manager or owner as mentioned above.

Telephone Systems

112. The law protects the privacy of telephone conversations. Without court approval, it is illegal to record or monitor audio or visual telephone conversations without advising the participants that the call is being monitored or recorded.
113. The use of RSN telephone equipment creates transaction records (which include the number called and the time and length of the call) that are reviewed by the RSN Senior Management Team and Departmental Heads as part of routine procedures.
114. Students are not granted access to any RSN telephone equipment under normal circumstances. If access is required for a specific purpose, approval is required from a departmental head or administrator.

Investigation and Response to IT violations

Policy

115. Instances of breaches may be drawn to the attention of the IT Manager and Senior Management Team via internal or external complaints, the intrusion detection system, or discovered in the normal course of business.
116. The actions taken because of a policy violation are dependent on the particular circumstances.

Immediate Response

117. The IT Manager will the impact of the alleged violation and take, without notice, any necessary action if RSN resources and services are adversely affected to prevent immediate and further damage to the RSN network. Such actions may include:

    Suspension of an account

    Disconnection of systems or disable network ports

    Termination of running processes and programs

    Any other actions deemed necessary to restore network services.

Investigation of Alleged Violations

118. The IT Manager (with assistance if required) will gather evidence and provide information as directed by the Senior Management Team or appropriate Heads of Departments to comply with any internal investigation. In some cases, the users may not be notified first or it may be required by law to provide the information without notifying the user. Investigations into complaints may necessitate the examination of systems and network activity logs and transaction logs. Contents of emails and other files will not be examined as part of a routine except in the following circumstances without the holder being notified:

    A court order requires that the content be examined and disclosed.

    The IT Manager is instructed in writing either by the CEO or Finance Director or Operations Manager or Board of Trustees as part of an internal investigation.

119. If the violation does not prevent other users from accessing network computer resources or result in a disciplinary procedure being instigated, the matter will be referred to the appropriate administrative authority for disciplinary action if the user refuses to comply.
120. Network access may be terminated immediately if the violation has been caused by an external entity with a contractual agreement with the RSN whilst the violation is investigated.

Reporting Security Incidents

121. All users of RSN IT Resources are encouraged to note and report any observed or suspected security incidents, security weaknesses in or threats to systems and services. Such reports can be made at the local campus helpdesks.

Disciplinary Action

122. Students whose actions contravene the guidelines within the RSN IT Policy or any of its related policies will find themselves subject to disciplinary proceedings as defined within the RSN's relevant student regulations.
123. Individuals in contravention of the RSN IT policy may also be subject to criminal proceedings. The RSN reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this Policy.

Appendix A

Guidance for students considering using external online technologies (third-party Internet and web 'cloud' service providers)

The RSN encourages students to make appropriate use of external Internet and Web technologies ('external online technologies') as long as adequate provision is made to ensure student and staff safety and privacy and minimise legal, operational, financial and reputational risk to the RSN.

These services offer attractive and useful applications services including file storage, portfolios, galleries, blogs, wikis, office systems, discussion forums, support services, social bookmarking and social networking.

However, before using such services—or expecting others to do so—students should appreciate the issues outlined below:

Advantages

External online technologies may offer the latest in functionality and support

They may be used by a great many people (e.g. Facebook, Adobe Creative Cloud, Youtube and Vimeo), making it easy to contact others and work together.

Account creation and access is normally very quick and cheap, if not free

They can help you to develop a professional portfolio of work for promotional purposes

Disadvantages

It is easy to add content to such sites that you might later regret, as many such sites own control and will not always allow you to delete comments you no longer wish to be associated with.

If you upload your work to an external service provider you may be giving up some of your copyright and granting the service provider ownership of your work. If in doubt, check the terms and conditions of the service provider.

Any content or comments you do submit can potentially become available to anyone in the world. It may also be unable for you to remove content and comments at a later date.

Such content may have a longer life span than you might have imagined and could be accessed by a wide audience, including potential employers.

It may not be possible for the RSN IT department or another authorised party to assist you with problems (e.g. loss of access to, or loss of, data).

Important!

Always read and consider the terms and conditions for any service you register with and ensure that you understand the implications of the service conditions.
Do not use the service for any RSN work unless you are happy with the terms and conditions; if you are in any doubt, ask your tutor or a department head or the IT Manager for clarification.

--- END OF DOCUMENT ---

Confidentiality Agreement

(Mutual Non-Disclosure Agreement)

THIS AGREEMENT is made on the _____ (**"Effective Date"**).

PARTIES:

(1) **ROYAL SCHOOL OF NEEDLEWORK** of **Apt 12a, Hampton Court Palace, KT8 9AU** and

(2) _____ of _____

WHEREAS:

The parties may have disclosed or wish to disclose to each other certain information of a confidential nature and wish to protect such information in the manner set out in this Confidentiality Agreement.

IT IS AGREED as follows:

1 DEFINITIONS

In this Agreement the following words and expressions shall have the meanings set out below:

"Confidential Information" means and includes:

(a) any information of whatever nature, including without limitation, documents, letters, plans, diagrams, sketches, drawings, photographs, storyboards, scripts, designs, proposals, concepts, processes, models, specifications, data and any other material bearing or incorporating any information relating to the Disclosing Party and/or its know-how, business, affairs, customers, suppliers and/or assets disclosed whether in writing, orally or by any other means by the Disclosing Party or a third party acting on its behalf, whether before, after or on the date of this Agreement;

(b) analyses, compilations, studies, notes and other documents prepared by the Receiving Party which contain or otherwise reflect or are generated from any such information as is specified in paragraph (a) above; and

(c) information of whatever nature obtained by observation during visits to premises;

but shall exclude any part of such disclosed information which (and which can be shown by documentary evidence):

(i) is or becomes available in the public domain without breach of this Confidentiality Agreement by the Receiving Party;

(ii) the Receiving Party can prove was lawfully in its possession, free of any restrictions as to its use or disclosure before the date of disclosure;

(iii) is received by the Receiving Party from any third party not acting on behalf of the Disclosing Party having the right to disclose such information; or

(iv) the Disclosing Party has given written approval to the Receiving Party for its disclosure by the Receiving Party.

"Disclosing Party" means whichever of the Parties together with its directors, employees, advisers, trustees, volunteers, partners, contractors and agents, which discloses Confidential Information to the other in connection with the Purpose;

“Purpose" means any suggested, discussed, proposed or agreed project (or projects), task (or tasks), advice, contract for goods, contract for services, trade, authorised information sharing or other requirement between the Disclosing Party and the Receiving party.

"Receiving Party" means whichever of the parties together with its directors, employees, advisers, trustees, volunteers, partners, contractors and agents, which receives Confidential Information from the other in connection with the Purpose;

References to statutes or statutory provisions shall include any statutory modification or re-enactment thereof.

2 OBLIGATIONS OF THE RECEIVING PARTY

2.1 In consideration of the Confidential Information being disclosed by the Disclosing Party, the Receiving Party undertakes that it shall:

2.1.1 use the Confidential Information solely for the Purpose and only disclose the Confidential Information to those persons who are required in the course of their duties to receive and consider the same;

2.1.2 treat and safeguard as private and confidential all of the Confidential Information and not by any means whatsoever disclose or allow access to Confidential Information (or permit such disclosure or access) to any person whatsoever without the prior written consent of the Disclosing Party and in strict accordance with the terms of such consent;

2.1.3 not without the prior written consent of the Disclosing Party copy by any means whatsoever any of the Confidential Information supplied or disclosed to it;

2.1.4 not make any inappropriate use of the Confidential Information or any part thereof;

2.1.5 procure that any of its advisers, contractors or agents to whom disclosure of any Confidential Information is to be made agree prior to such disclosure, to be bound by the obligations in this Confidentiality Agreement as if they were a party hereto and the Receiving Party shall be responsible for any breach of such obligations as they apply to such persons;

2.1.6 procure that any of its directors, partners, trustees, employees or volunteers to whom disclosure of the Confidential Information is to be made, agree to honour the obligations set out in this Confidentiality Agreement; and

2.1.7 not reveal to any person other than as permitted by clause 2.1.5 or make any public announcement:

2.1.7.1 of the fact that any investigations or discussions are taking place concerning the Purpose;

2.1.7.2 that either party has requested or received any Confidential Information; or

2.1.7.3 of any terms or conditions or of other facts relating to the Purpose, or to its status.

2.2 The Receiving Party shall within 14 days of receipt of a written request from the Disclosing Party:

2.2.1 return to the Disclosing Party all physical Confidential Information provided by the Disclosing Party that is in the Receiving Party’s possession or under the Receiving Party’s custody and control and all copies thereof and, so far as it is practicable to do so but in any event without prejudice to the obligations of confidentiality contained herein, expunge any Confidential Information from any computer, word processor or other device in the Receiving Party’s possession or under the Receiving Party’s custody and control; and

2.2.2 destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by the Receiving Party or the Receiving Party’s advisers, which contain Confidential Information or in which Confidential Information is incorporated and shall on request, deliver to the Disclosing Party a certificate signed by any director having satisfied himself that to the best of his knowledge, information and belief the provisions of this clause have been complied with.

3 GENERAL

3.1 Notwithstanding the provisions of clause 2, the Receiving Party shall be entitled to make any disclosure of the Disclosing

Party's Confidential Information required by or essential to comply with any law or the requirements of any government or regulatory authority acting within the scope of its powers, provided that it gives the Disclosing Party as much notice as is reasonably practicable prior to such disclosure. The Receiving Party shall take all the necessary measures at its expense to limit the Confidential Information disclosed to the minimum required.

3.2 Each party shall be fully and solely responsible for instituting, maintaining, implementing and enforcing all security or other measures to comply with its obligations under this Confidentiality Agreement.

3.3 Either party shall not take any action in relation to the Purpose and the Confidential Information, which shall or may cause the other party to be in breach the Data Protection Act (2018), the Computer Misuse Act (1990), the Copyright Designs and Patents Act (1988) or the Human Rights Act (1998).

3.4 Any Confidential Information supplied or disclosed shall remain the property of the Disclosing Party.

3.5 None of the Confidential Information has been subject to verification, and neither the Disclosing Party nor any of its advisers accepts responsibility for, or makes any representation, express or implied, nor does the Disclosing Party give any warranty with respect to the accuracy or completeness of the Confidential Information or any oral communication in connection therewith, and the Receiving Party hereby undertakes to the Disclosing Party to waive any liability which may be incurred by reason of the Receiving Party's use of, or reliance upon, any of the Confidential Information.

3.6 This Confidentiality Agreement is personal to the parties and may not be assigned, unless both parties agree in writing.

4 REMEDIES

4.1 Without prejudice to any other rights or remedies which either party may have, each party acknowledges and agrees that damages would not be an adequate remedy for any breach by the other party of the provisions of this Confidentiality Agreement and the aggrieved party shall be entitled, without proof of special damage, to the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of any such provision by the other party.

5 TERMS AND NOTICES

5.1 This Confidentiality Agreement shall remain in force without limit in time unless otherwise agreed by mutual written consent.

5.2 All notices served by either party under this Confidentiality Agreement shall be in writing, sent by facsimile or first-class registered or recorded delivery post to the address of the relevant party as set out at the beginning of this Agreement.

6 SEVERABILITY

6.1 If any term or provision in this Confidentiality Agreement shall be held to be illegal or enforceable, in whole or in part, under any enactment or rule of law or otherwise, such term or provision (or part thereof) shall to that extent be deemed not to form part of this Confidentiality Agreement but the enforceability of the remainder of this Confidentiality Agreement shall not be affected.

7 GOVERNING LAW

7.1 This Confidentiality Agreement shall be governed by and construed in accordance with the laws of England and Wales and each of the parties hereto submit to the exclusive jurisdiction of the Courts of England and Wales.

AS WITNESS this Confidentiality Agreement has been signed on behalf of each party by its duly authorised Representatives.

Signed for and on behalf of	Signed for and on behalf of
ROYAL SCHOOL OF NEEDLEWORK	_____
Signature _____	Signature _____

Name _____ Name _____

Date _____ Date _____

GDPR

General Data Protection Regulation

Approved by RSN Council on DATE

For review byPWG
September 2022

To be read in conjunction with the following relevant Policies:
Privacy Policy – August 2018
Document retention policy

Please contact the policy owner if you have a query: Scott Bartlett

This policy reflects legislation and official guidance at the time it was last reviewed.
Any changes in legislation will take precedence over anything printed in this policy.
Where other policies are referred to they can be viewed at Policy Library

GDPR

Links with other school policies and practices

This policy links with the following other RSN policies and practices:

- Privacy Policy – August 2018
- Institutional agreement between Kingston university higher education corporation and Royal School of Needlework - February 2022
- Document retention policy – to be collated from existing information - TBD
- Digital and Cyber security policy – TBD
- Freedom of information - TBD

1. Introduction

1.1. As an organisation which collects and processes personal data the RSN has to comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The EU's GDPR has been lifted into a new UK-GDPR (United Kingdom General Data Protection Regulation) that took effect on January 31, 2020.

1.2. This policy forms part of any employee's contract of employment.

1.3. This policy seeks to ensure that we:

- Have clarity about how personal data must be processed and the RSN's expectations for all those who process personal data on its behalf;
- Comply and are able to demonstrate compliance with the data protection law and good practice;
- Protect the RSN's reputation by ensuring the personal data collected is processed in accordance with data subjects' rights
- Protect the RSN from risks of personal data breaches and other breaches of data protection law.

1.4 This policy represents the minimum we expect from our workforce and others involved in the RSN. If applicable law requires a higher standard or additional requirements, then these must be adhered to.

2. Scope

2.1 The Policy and Procedure set out in this document applies to the RSN Workforce, Council members and volunteers. (see definition of workforce Appendix 1).

3. Accountability

3.1. The RSN will implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The RSN is responsible for and must be able to demonstrate compliance with data protection principles.

- We will apply adequate resources and controls in ensuring we document GDPR compliance including:
- Appointing a suitably qualified Data Protection Officer (DPO);
- Implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where

processing presents a high risk to the privacy of data subjects; (note this is likely to be very rare)

- Integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;
- Training the workforce, Council members and volunteers on compliance with Data Protection Law and keeping a record accordingly; and
- Conducting periodic reviews and audits to assess compliance,

4. Roles and Responsibilities

4.1. Responsibilities

As the Data Controller, the RSN is responsible for establishing policies and procedures in order to comply with data protection law.

There must be a designated (DPO) who has the following responsibilities;

- Advising the RSN and its workforce of their obligations under GDPR
- Monitoring compliance with this Regulation and other relevant data protection law, RSN's policies with respect to this and monitoring training and audit activities relating to GDPR compliance
- To provide advice where requested on DPIA
- To cooperate with and act as the point of contact for the Information Commissioner's Office
- The post holder will in the performance of his or her tasks have due regard to the risk associated with data processing operations, taking into account the nature, scope, context and purposes of processing.

4.2 Workforce responsibilities

Member of the workforce who process personal data about customers, current and former employees, donors, free-lance tutors, contractors or any other individual must comply with the requirements of this policy. They must ensure that:

- All personal data is kept securely;
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data is kept in accordance with RSN's retention schedule;
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO;
- Any data protection breaches are swiftly brought to the attention of the DPO;
- Where there is uncertainty around a data protection matter advice is sought from the DPO;
- Where employees are responsible for supervising service users doing work which involves the processing of personal information, they must ensure that those service users are aware of the Data Protection principles.

Workforce members who are unsure about which third parties they can legitimately share personal data with should seek advice from the DPO.

4.3 Third-Party Data Processors Where external companies are used to process personal data on behalf of the RSN, responsibility for the security and appropriate use of that data remains with the RSN.

- Where a third-party data processor is used:
    - The data processor chosen must provide sufficient guarantees about its security measures to protect the processing of personal data;
    - Reasonable steps must be taken to ensure appropriate security measures are in place;
    - A written contract should be set out establishing what personal data will be processed and the purpose for processing;
    - A data sharing agreement must be signed by both parties.
    - For further guidance about the use of third-party data processors please contact the DPO.

4.4 Contractors, Free-Lance tutors, Temporary Staff, Agency Staff and Volunteers

- The RSN is responsible for the use of personal data by anyone working on its behalf. Managers who employ contractors, temporary or voluntary staff, free-lance tutors and agency staff must ensure that they are appropriately skilled to handle the data they will be processing. In addition managers must ensure that:
    - Any personal data collected or processed in the course of work undertaken for the RSN is kept securely and confidentially;
    - All personal data is returned to the RSN on completion of the work, including any copies that may have been made. Alternatively ensure that the data is securely destroyed and the RSN receives notification in this regard from the contractor or short term staff / volunteers;
    - the RSN receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
    - Any personal data made available by the RSN, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the RSN;
    - All practical and reasonable steps are taken to ensure that contractors, short term staff or volunteers do not have access to any personal data beyond what is essential for carrying out their role.

4.5 Service User's responsibilities are as follows:

- Familiarising themselves with the Privacy Notice provided when they become service users;
- Ensure any personal data provided to the RSN is accurate and up to date.

5. Principles

The processing of personal data collected by the RSN is guided by the following principles as set out in the GDPR. The RSN is responsible for and must be able to demonstrate compliance with the data protection principles set out below:

- Lawfulness, fairness and transparency - Personal data is processed lawfully, fairly and in a transparent manner.
- Purpose Limitation - Personal data is collected only for specified, explicit and legitimate purposes and not processed further in a manner incompatible with those purposes.
- Data Minimisation – Personal data collected is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accuracy – Personal data collected is accurate and where necessary kept up to date.
- Storage Limitation – Personal data collected is not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed.
- Security, integrity and confidentiality – Personal data collected is processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

For further details on these principles refer to the ICO Guide to GDPR available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

6. Rights of a Data Subject

A data subject has rights in relation to the way we handle their personal data. Data subjects have the right to:

- withdraw consent for processing their data at any time where the legal basis for processing their data is consent;
- ask for access to the personal data that is held (Subject Access Requests);
- prevent the use of their personal data for direct marketing purposes including profiling
- object to the processing of their personal data in limited circumstances
- erasure of their personal data without delay: If it is no longer required in relation to the purposes for which it was collected or otherwise processed;
- data portability which allows data subjects to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

7. Data Subject Access Requests

Data subjects have the right to receive a copy of any personal data held by The RSN. This must be **no later than one calendar month, starting from the day the RSN receives the request.** In addition, an individual is entitled to receive further information about the RSN's processing of their personal data as follows:

- The purpose for which personal data is processed
- The categories of personal data that are processed
- Recipients/categories of recipients
- The retention periods for categories of personal data
- Information about data subject's rights
- The right of a data subject to make a complaint to the ICO,
- Details of the relevant safeguards where personal data is transferred outside the UK?

Do not allow third parties to persuade you into disclosing personal data without proper authorisation. For example, service user's parents do not have an automatic right to gain access to their son's or daughter's data.

- The right relates to personal data held electronically and to limited manual records. It is not an entitlement to documents specifically, because this may be accessed through the Freedom of Information Act, subject to any exemptions and the public interest criteria.
- You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact the DPO before any changes are made to personal data which is the subject of an access request.

8. Reporting a personal data breach

The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We will notify data subjects or the ICO where we are legally required to do so.

If it is known or suspected that a personal data breach has occurred, it should immediately be reported to the DPO and the instructions in the personal data breach procedure must be followed. All evidence relating to personal data breaches must be retained in particular to enable the RSN to maintain a record of such breaches, as required by the GDPR.

9. Limitations on the transfer of personal data

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. However, as part of the Brexit negotiations an agreement has been reached to maintain data transfer protocol between the UK and EU in line with pre Brexit agreement. This means the UK is deemed to be a safe country for the purposes of personal data transfers for four years. The transfer of personal data originating in one country across borders occurs when you transmit or send that data to a different country or view/access it in a different country.

If data is to be transferred out of the EU the DPO should be consulted and appropriate professional advice obtained.

10. Record Keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' consents and procedures for obtaining consents where consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of The RSN as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

- The facts surrounding the breach
- Its effects; and
- The remedial action taken

Appendix 1

Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated processing.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual. In particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

Data Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the GDPR. RSN is the Data Controller of all personal data relating to it and used delivering services, donations and all other purposes connected with it including business purposes.

Data Processor A processor is responsible for processing personal data on behalf of a controller.

Data Subject: a living, identified or identifiable individual about whom we hold personal data.

Data Protection impact assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person appointed as such under the GDPR and in accordance with its requirements. A DPO is responsible for advising the RSN (including its workforce) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the RSN's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Personal Data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an

individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to data subjects when the RSN collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee, service users and donor privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose. (c.f. RSN's Privacy Notice).

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so the person to whom the data relates cannot be identified without the use of additional information. That additional information is meant to be kept separately and secure.

Sensitive data, or special category data, according to GDPR is any data that reveals a subject's information. Sensitive data examples: Racial or ethnic origin, political beliefs, or religious beliefs. (RSN do not currently collect this information).

Service Users, those people using RSN services, including customers, students, volunteers, future tutors, tutors, free-lance teachers, donors, and contractors.

Workforce For the purpose of this policy 'workforce' means an employee who receives direct payment from the RSN for work carried out on its behalf, it includes anyone working on contract or agreement for the RSN in the delivery of RSN services, including free-lance teachers.