Regulations for the Use of IT Facilities

Version 10.0

Approved by the Board of Governors

Last reviewed: August 2026

The following regulations outlines the constraints and practices relating to acceptable use of the School's IT facilities, including desktop computers, laptops, printing facilities and internal networks. It expands upon the Employee and Student Codes of Conduct, and is to be followed by all staff members and students.

These regulations have been drafted with due regard for the relevant information security laws, namely:

i. *Computer Misuse Act 1990*
ii. *UK GDPR and the Data Protection Act 2018*

Furthermore, the School recognises the importance of monitoring and regulating IT the use of IT facilities in upholding its Prevent duty.

These regulations are non-contractual and may be amended from time to time to meet the operational needs of the School.

DOCUMENT INFORMATION

Document owner(s)*: IT Department

Date of next review: September 2027

Document Status: IN USE

Dissemination: The following is for general publication and should be made available to students and staff members on induction.

*The document owner is responsible for maintaining and updating the content of this document and ensuring that it reflects current practice at the School.

Contents

DOCUMENT INFORMATION 1
1. ABOUT THE REGULATIONS 2
2. SECTION A 2
2.1. Examples of Unacceptable Use of IT Facilities 2
2.2. Rules Regarding Use of IT Hardware 3
2.3. User Accounts and Login Credentials 4
2.4. Data Protection and IT Security 4
3. SECTION B: APPLICABLE TO EMPLOYEES ONLY 5
3.1. Emails and Instant Messaging 5
3.2. Access Rights and Permissions 6
3.3. Use of Portable Data Devices 7
3.4. Use of School Software and Work Applications 8
3.5. Remote Working 8
3.6. Internet Browsing at Work 9
3.7. Review of These Regulations 10
VERSION HISTORY 11

1. ABOUT THE REGULATIONS

1.1. The purpose of these regulations is to ensure that employees and students are aware of the School's expectations when using its IT facilities in order to prevent their misuse leading to breaches of School policies; regard is given in particular to upholding the School's *Data Protection Policy*.

1.2. Where IT users should fail to observe these regulations, the consequences can potentially be severe for the employee and for the School. The School must therefore treat any actual, attempted or suspected infringement of these regulations seriously and may take disciplinary action against anyone acting or attempting to act in breach of it; in the most serious cases such action may include dismissal without notice for gross misconduct or expulsion from a programme of study.

1.3. These regulations are not intended to inhibit in any way the academic freedom of LSST's staff and students to engage in legitimate research activities relating to curriculum delivery; any access to online subject matter which would usually be prohibited by these regulations may be permissible with authorisation sought in advance from senior academics and network administrators.

1.4. The Regulations are split into **Section A** and **Section B:**

- **A** deals with regulations applicable to employees and students.
- **B** deals with regulation applicable solely to employees.

2. SECTION A

2.1. Examples of Unacceptable Use of IT Facilities

2.1.1. The School will not tolerate any instances of students or employees:

i. Using School IT facilities in such a way that causes financial, material or reputational harm the School and/or those affiliated with it, for example by:

- Unauthorised sharing of sensitive, confidential or strategic information.
- Unofficially publishing personal views and values as those of the School.
- Intentionally or unintentionally exposing School systems to malware (such as computer viruses) or other electronic security threats.
- Causing damage to hardware and IT equipment.

(The above list is not exhaustive).

ii. Using IT facilities in any way that would constitute bullying, harassment and/or victimisation of a person (as set out in the School's Prevention of Bullying, Harassment, and Sexual Misconduct Policy).

iii. Viewing, creating, sharing or distributing unlawful material or messages such that may be construed as libellous, defamatory threatening or extremist in content, or material which advocates breaking the law or in any way breaches the School's Prevent Duty policies.

iv. Viewing, creating, sharing or distributing material which would be considered "Not Suitable for Work" (or "NSFW"); this refers mainly to material containing nudity, explicit sexual references, profanity, violence, and/or other potentially disturbing subject matter).

v. Attempting to gain access to another employee's or student's IT user account in order to act on behalf of that person, whether with or without their consent.

vi. Downloading or disseminating copyright materials without the permission of the copyright owner.

vii. Downloading or playing computer games.

2.1.2. Students and employees should exercise discretion in sending humorous material or jokes to colleagues over School networks and are advised to refrain from doing so, as material which they find acceptable might be offensive to others, and that even if the intended recipient is not offended by the message, it may be forwarded on to a person who is, in which case the original sender may be held to account.

2.1.3. Employees should not send humorous material or jokes to external parties as these may be misunderstood or cause offence; this behaviour does not align with LSST's standards of professional conduct.

2.2. Rules Regarding Use of IT Hardware

2.2.1. The following relates to treatment of the School's IT hardware (including computers, laptops, phones/smartphones, display screens/projectors, printer copiers, etc):

i. No IT equipment may be moved without the consent of the IT Department (with the exception of small items such as desktop phones, conferencing hubs and cables), and in such circumstances the IT Department will carry out the move.

ii. No equipment may be attached to the School's network without the consent of the IT Department and in such circumstance the IT Department will carry out the attachment.

iii. No equipment may be modified without the consent of the IT Department and in such circumstance the modification will be made by the IT Department.

iv. All School IT equipment must be treated with care and left in good working order. Any fault, loss or damage must be reported by an employee to their Line Manager, as well as the IT Department immediately.

v. All equipment must be logged-off correctly and powered down when not in use for long periods of time; employees must turn off their PC at the end of each working day.

vi. School-issued laptops, tablet computers and mobile phones must be kept secure when taken off site and never left unattended in a public place. Employees are

required to take all reasonable measures to minimise the risk of loss or theft occurring to School equipment and data.

vii. It is mandatory that employees re-boot their computer daily to enable periodic system updates, including important security updates, to take effect.

2.3. User Accounts and Login Credentials

2.3.1. All students and employees will be assigned a personal IT user account with specific login credentials (i.e., username and password) shortly after starting with the School, which can be used to log on to any computer connected to the School's network. A person's IT user account is for their use only; employees and students should take all reasonable steps to prevent unauthorised use of their user account by anyone other than themselves.

2.3.2. Individuals will be held responsible for all actions undertaken on a system which has been logged onto with their username and password, regardless of whether those actions were their own.

i. User account passwords are to be kept confidential and must not be shared with anyone. Employees and students should refrain from writing their password down in a place where it could be seen by anyone else.

ii. A logged-in workstation should never be left unattended; employees and students should always log out of or lock their workstations when not working at them to prevent unauthorised use.

iii. Where any employee/student suspects their login details may have been compromised, they should immediately notify their Line Manager/Administration Officer, who will request the IT Department to change them.

iv. Employees gaining or attempting to gain unauthorised access to another employee's user account in order to view or edit files they should not have access to, or present themselves as another staff member, will be subject to disciplinary action which may lead to summary dismissal for gross misconduct.

v. Where Multi-Factor Authentication (MFA) is enabled on a user account, employees and students must not disable it, decline to enrol a second authentication factor, or share access to their MFA device or authentication codes with any other person. MFA approval requests must only be accepted by the account holder personally; approving an MFA request on behalf of, or at the instruction of, another individual is strictly prohibited and will be treated in the same manner as unauthorised account sharing under clause iv, and may lead to disciplinary action up to and including summary dismissal for gross misconduct.

2.4. Data Protection and IT Security

2.4.1. Employees and students must take reasonable steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data.

2.4.2. Anyone who suspects their computer, or any other workstation, may be infected with malware (such as a computer virus) must report the matter to their line manager or course leader and comply with the directions of the IT Department. Failure to do so

can jeopardise the security of the School's computer network and could result in data loss/damage to computer hardware and software.

2.4.3. All attempts to circumvent the School's IT Security protocols, either deliberately or otherwise will be investigated by the IT Department and appropriate action will be taken. Examples of such actions would include disabling network firewalls, use of proxy servers to browse restricted websites, installation of software via 'back-door' methods, disabling security software, etc. Depending on the severity, such acts may lead to immediate dismissal for gross misconduct or expulsion form a programme of study.

2.4.4. Email file attachments should not be opened unless they are received from a trusted source, *i.e.,* from another known School, employee or student or student representative. If in doubt, recipients should forward the email to the IT Department for verification.

2.4.5. All LSST staff, students, and authorised third parties must enable and maintain Multi-Factor Authentication (MFA) on all LSST IT systems and accounts where MFA is supported, including but not limited to email, Microsoft 365 and any system used to store or process personal or sensitive data. Users must not disable, bypass, or otherwise attempt to circumvent MFA controls without prior written authorisation from the IT Department. Any attempt to circumvent MFA will be treated as a breach of this Regulation and investigated in accordance with clause 4.3, and may result in suspension of system access and/or disciplinary action, including expulsion from a programme of study or dismissal for gross misconduct, depending on severity.

3. SECTION B: APPLICABLE TO EMPLOYEES ONLY

3.1. Emails and Instant Messaging

3.1.1. The School's email and other internal communications platforms are to be used only for legitimate business purposes. All written communications sent over School servers are recorded and archived and may be viewed by the School at any time. Employees should therefore be mindful of the following when sending emails or personal messages from their user account.

i. The tone of all communications made via email, IM or CRM should be appropriate and professional; messages should never be of a hostile nature, use rude, inappropriate or threatening language or contain profanities.

ii. Communications should be proof-read and spellchecked, particularly where they sent in an official capacity to external recipients; this is to prevent ambiguity or misinterpretation arising, whilst preserving standards of professionalism.

iii. Emails sent to external networks will display a School footer, employees should not add their own footers or signatures to outgoing emails.

iv. It is accepted that Instant Messages between colleagues may be of a less formal nature; employees should nonetheless use their discretion when considering what would be an acceptable tone to use over the School's IM platform.

v. The School does not permit the use of its email for unofficial and/or personal purposes, including social invitations, personal messages, jokes, chain letters or

other private matters, although this may be permissible in exception circumstances and with a Line Manager's permission.

vi. Emails to customers, suppliers and other business contacts should only relate to business matters. Confidential or sensitive information relating to the School or its employees should not be transmitted via email unless done so in the course of business and with a Line Manager's approval; where there is any doubt about whether certain information should be disclosed, the School's Data Protection Officer should be consulted.

vii. Email messages should only be sent to those for whom they are particularly relevant; the sender should refrain from copying in long lists of people who are peripheral to or not involved in the matter under discussion.

viii. Further to (vii.); employees should be aware that, as an email thread develops, it may no longer be appropriate to copy in people originally included, as this may be a distraction to those no longer involved or potentially result in disclosure of information to the wrong person(s).

ix. All internal communications are presumed confidential, and a communication which is exclusively between School employees must not be forwarded to external recipients (including consultants) unless it has been marked as "approved for external distribution" and/or specific agreement has been sought and received from the most Senior Manager copied in to such e-mail.

x. Employees who receive any email or personal message that is not intended for them should immediately notify the sender of the error and delete the message from their inbox to preserve confidentiality.

xi. Where unusual circumstances require an employee to use a non-School email address, the employee must seek the approval of their Line Manager for such usage, forward all messages sent and received by their personal account to the Line Manager, promptly delete all copies their personal email account once access to their School email is restored.

xii. Employees should not knowingly attach to emails, any files which may contain a virus, malware or spyware as the School could be liable to the recipient for any loss suffered by them as a result.

xiii. Employees should take care that there is no infringement of copyright when adding attachments to emails.

3.1.2. Further to the above the School may from time-to-time update employees with additional guidance on email etiquette and formalities; employees will be expected to exemplify this guidance in their correspondence.

3.2. Access Rights and Permissions

3.2.1. The access permissions assigned to an employee's user account will allow them to view only files, folders and directories that are relevant to their field of work, as per the approval of their Line Manager. Similarly, employees' access credentials may extend their access to School databases and Client Relations Management (CRM) platforms and special email boxes; again, the extent of access will be determined by the conditions attached to that employee's user account.

i. Employees requiring access to School files, datasets, applications or mailboxes in order to fulfil a work function should first seek permission from their Line Manager before forwarding that permission to the IT Department to process the request.

ii. All requests to the IT Department should clear about the extent and type of access (i.e., editing rights/read-only, etc.) required.

iii. Employees must not attempt to circumvent access restrictions; to do so may be construed as gross misconduct and result in summary dismissal.

iv. Where new access permissions would potentially grant an employee access to data defined as 'sensitive', 'personal' or 'special category' information within the School's Data Protection Policy, the IT Department may first query the request with the School's Data Protection Officer (DPO); in this instance the employee and their Line Manager may need to justify the request for access in relation to the work function.

v. Employees who no longer require access to certain folders, directories, databases, etc. should relinquish this access as soon as possible by contacting their Line Manager and forwarding a request to the IT department as soon as possible.

3.3. Use of Portable Data Devices

3.3.1. The following relates to the security of any electronic School data which is physically separate from the School's networks; this might be information on portable storage media such as USB memory sticks (pen drives), DVDs and external hard drives, or it on portable computing devices such as laptops, tablet computers or phones.

i. Employees must not use portable storage media to transfer files between School computers; this should be done using the network drives and/or Intranet.

ii. School data should be loaded onto portable storage media only in urgent and/or exceptional circumstances with permission sought in advance form a Line Manager; all files should be removed from the device immediately once they are no longer needed and returned to a location on the School's network or deleted.

iii. Employees transporting a portable data device with School information on it, whether on or off of School premises, should ensure the device is securely in their possession at all times; the device must never be left unattended (e.g. plugged into a computer workstation or left in an unlocked draw).

iv. Files stored on a portable device should be password protected and/or encrypted as per the requirements of the IT Security Policy.

v. In the event that a laptop or other portable data device has been lost or stolen, this must be reported immediately to the appropriate Line Manager and the IT department; the Data Protection Officer should also be informed about any sensitive School or personal data on the device and the implications the loss of this data may have.

vi. Employees who receive media from any unknown source must have it virus checked by the IT Department. Employees bringing in media from a home computer must get permission from the IT Department before doing so.

3.4. Use of School Software and Work Applications

3.4.1. Employees' workstations will be set up by the IT Department and must not be altered by the user. This setup will include installation of any specific programmes and applications required by the employee to perform their role.

i. Under no circumstances will employees be permitted to purchase or load any unauthorised software without approval from their Line Manager and the IT Department. If a specific application programme is necessary for an employee's work, then the School will consider its purchase, and where approved, the IT Department will manage the download and installation.

ii. Standard operating procedures must be followed at all times when using software. Where no procedures exist, employees should consult with the IT Department and follow any instructions given.

iii. All original software, disks or CD/DVD ROMs, or USB installers should be kept with the IT Department; employees in possession of any software on physical media formats should provide these to the IT Department as soon as possible.

iv. It is illegal to make unauthorised copies of software or use third party applications without lawfully obtaining the proper licenses. Software and computer facilities issued by the School for employees' use are licensed to the School and are protected by copyright law. Employees must not make copies of or distribute software that has been copied nor should they attempt to use unlicensed software applications. Employees who breach this condition will be subject to disciplinary action which could result in dismissal without notice for gross misconduct. Furthermore, persons who are found to making unauthorised duplicates of copyrighted software may be personally liable to prosecution under Copyright.

3.5. Remote Working

3.5.1. Even where employees are authorised to work, these regulations must be followed in full.

3.5.2. Employees may, if working remotely, use their own personal IT devices to do so, except where such work involves the control or processing of personal data or confidential or strategically sensitive company information; under no circumstances may employees transfer such data to their personal devices.

3.5.3. The School will not usually permit the connection of personal devises to networks which contain protected information; restricted access may be permitted at the discretion of line managers, the School's Data Protection Officer and the Head of IT.

3.5.4. The School may additionally prohibit the transfer of its intellectual property onto employees' personal devices, where such intellectual property is not already in the public domain.

3.5.5. Employees must consult with their Line Manager, the College's Data Protection Officer and the Head of IT prior to agreeing any remote working arrangements.

3.5.6. Employee must not use their personal or 3rd party VPN under any circumstance and access the company Data unless it is authorised by the Head of IT.

3.5.7. Any unauthorised VPN connection attempting to access the School's network or data will be automatically blocked and reported to the IT Department, and the individual responsible will be investigated in accordance with clause 4.3 of the Data Protection and IT Security policy. Depending on the severity of the breach, this may result in disciplinary action up to and including summary dismissal for gross misconduct.

3.6. Internet Browsing at Work

3.6.1. Employees should note that the School reserves the right to monitor employees' use of its internet facilities and maintains a record of individual user's internet histories. Line Managers will be able to request a report on an employee's online activities whilst at work on a School computer where they may have concerns about the amount of time an employee spends online and/or the web content viewed.

3.6.2. Employees may at any time be called upon to justify the amount of time which they have spent on the Internet, or on any specific Internet site, during working hours.

3.6.3. The following outlines that which constitutes acceptable use of School Internet access:

i. All School computers have Internet access which is provided for business purposes only; employees personal internet browsing, or correspondences should be conducted during designated breaks and preferably on their own personal devices.

Note: Whilst at work, employees are still required to comply with the general provisions in Section 1 of this Code, regardless of whether they are using their own personal devices.

ii. Under no circumstances may any employee download any files from the Internet; this should only be done by the IT Department and with the written consent of their Line Manager.

iii. Anyone believed to have been viewing unsuitable content as defined in Section 1 - iv. will be subject to disciplinary action. Offences of this nature may be considered gross misconduct and lead to dismissal without notice.

Note: The School subscribes to internet 'reputation engines' which prevent access to websites material considered be unsuitable for the work environment; this includes (but is not limited to) NSFW materials, sites linked to criminal activity or hate speech, gaming and gambling sites.

Whilst 'reputation engines' are highly effective at blocking prohibited material there is no assurance that all NSFW results will be blocked from an internet search; if content is not filtered out this does not mean it is acceptable to the School and employees may be held to account for the web content, they view during work hours and/or using School IT facilities.

iv. Employees must not enter into any licence or contract terms via the Internet on behalf of the School, without the prior express consent from the School.

3.7. Review of These Regulations

3.7.1. The School's IT Department shall be responsible for reviewing this Policy to ensure that it meets all applicable legal requirements and reflects best practice.

3.7.2. Changes to these regulations will be approved by the School's Board of Governors.

VERSION HISTORY

Versions	**1.0 – 3.0**	
Original author(s):	Head of IT	
Reviewed by:	Executive Committee	September 2016 September 2017 September 2018
Version	**4.0 – 4.1**	
Revised by:	Quality Audit Manager Legal Advisor	
Revision summary:	*Expanded content and added 'Acceptable Use' definitions; alignment with Prevent Duty and Data Protection requirements; division into two sections; document reformatted and version control added. Endorsed by Publications Committee and the Executive for ratification by the Board of Governors.*	
Approved by:	Board of Governors	September 2019
Version	**4.2**	
Revised by:	Quality Unit Head of IT	
Revision summary:	*Annual review and update.*	
Approved by:	Board of Governors	October 2020
Version	**5**	
Revised by:	Quality Unit Head of IT	
Revision summary:	*Annual review and update.*	
Approved by:	Board of Governors	October 2021
Version	**6**	
Revised by:	Quality Unit IT Manager	
Revision summary:	*Annual review and update.*	
Approved by:	Board of Governors	September 2022
Version	**6.1**	
Revised by:	IT Department	
Revision summary:	*Document owner changed.*	
Approved by:	Board of Governors	March 2023
Version	**7**	
Revised by:	IT Department	
Revision summary:	*Annual Review; version control applied*	
Approved by:	Board of Governors	October 2023
Version	**8**	

Revised by:	IT Department Quality Unit	
Revision summary:	*Annual review and update, minor grammatical corrections, document format applied, version control applied.*	
Approved by:	Board of Governors	October 2024
Version	**9.0**	
Original author(s):	Head of IT IT Department	
Revised by:	Quality Unit	
Revision summary:	*Annual review and update –* *Paragraph 9.6 added. Minor grammatical corrections, document format applied, version control applied.*	
Reviewed by:	Publications Committee	September 2025
Approved by:	Board of Governors	October 2025
Version	**9.1**	
Original author(s):	Head of IT IT Department	
Revised by:	Quality Unit	
Revision summary:	*UK GDPR and Data Protection Act 2018 referenced on page 1 to reflect updated legislation. Version control applied.*	
Reviewed by: Approved by:	Publications Committee Board of Governors	February 2026 February 2026
Version	**10.0**	
Original author(s):	Head of IT IT Department	
Revised by:	Quality Unit	
Revision summary:	***Annual review and update –*** *Paragraphs 2.3.2.v. and 2.4.5. added on employee and student responsibilities regarding Multi-Factor Authentication (MFA). Paragraph 3.5.7. added on unauthorised VPN connections. Minor grammatical corrections, document format applied, version control applied.*	
Reviewed by:	Publications Committee	October 2026
Approved by:	Board of Governors	October 2026