

<b>Policy Name</b>	<b>Staff Acceptable Use Policy</b>
<b>Policy Number</b>	T035
<b>Date of Issue</b>	July 2023
<b>Date of next review</b>	July 2025

**Notes:**

This policy should be read in line with appropriate GDPR, IT and Safeguarding policies and procedures with reference to the Cyber Security Guidelines.

## 1. Scope of Policy

This Acceptable Use Policy (AUP) applies to all Landau Forte Charitable Trust Staff employed in any of its Academies or central functions, including any cover staff, temporary staff, associate staff, contractors and visitors. The agreement applies to anyone accessing any part of the Landau Forte systems whether onsite or remotely from offsite.

As an employee/representative of Landau Forte, you may have access to confidential and potentially sensitive information stored on the network and systems. You may also have access to portable devices supplied to you by Landau Forte such as laptops, tablets and smartphones/phones. You are responsible for any Landau Forte equipment in your care including your user account and email, their contents and activity.

### **You should not under any circumstances:**

- Access, store, distribute or print material from any medium which:
  - a) may bring the Landau Forte name into disrepute
  - b) may compromise the safety of Landau Forte, its students or employees
  - c) may be deemed offensive to your colleagues
  - d) is considered to be illegal or inappropriate
  - e) may breach Safeguarding or GDPR policies
  - f) was not intended for you
- Install, copy or bring into Landau Forte software which is not correctly licensed for use.
- Allow anyone else to access your user account, email, intranet or internet services.
- Allow anyone else to know your passwords.
- Change any computer files that do not belong to you or that you do not have access to.
- Plagiarise work without acknowledging the source.
- Use portable devices for taking images of individuals without prior consent.

Landau Forte provides internet and email access to all staff which has a filtering service that attempts to block illegal, unwanted and potentially offensive material. Content which passes these filters is not necessarily deemed to be acceptable by Landau Forte.

If you find any material which is inappropriate, offensive, illegal, controversial, or which is generally not suitable for staff or students to access, contact the Systems Support Team and the Designated Safeguarding lead who will take the appropriate steps. Do not attempt to take action yourself.

**You are allowed to use the Landau Forte Internet and Email system for personal use outside of contracted hours, but you should not:**

- Use the internet or email for any illegal or inappropriate purpose.
- Engage in any online activity that may compromise your professional responsibilities.
- Use impolite or abusive language.
- Violate the rules of common sense and etiquette.
- Send or receive copyright materials without permission.
- Use the Internet to bring into Landau Forte, in any form, materials that would be unacceptable on paper.

**You must:**

- Only use the approved, secure email system for any Landau Forte business.
- Only use the approved Landau Forte email, VLE or other approved communication systems with students or parents/carers, and only communicate with them on appropriate business.
- Ensure that any private social networking sites/blogs/twitter accounts etc that you create, or actively contribute to, are not confused with your professional role. NB: access to Social Networks, e.g. Facebook, and personal email accounts is prohibited during your contracted hours.

**If you need to use personal equipment on the Landau Forte network (e.g. you are an MFL Assistant and need your own laptop as it is in your native language) ensure that:**

- It does not contain material which is deemed unsuitable or inappropriate, as outlined above.
- It has an antivirus checker installed, with the latest updates applied.
- You do not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission, and also not store images at home without permission.

**Landau Forte reserves the right to:**

- View user's email.
- View user's internet usage/history and where necessary, interrogate and analyse that information.
- View any files stored in user areas or shared areas on the Landau Forte Network.
- View any material on Landau Forte owned equipment and to take appropriate action if these files contravene the policy as detailed above.

If Landau Forte require access to any of the above for specific individuals, this request will be actioned by a member of the IT team and before they are able to access any information, the request must be approved in writing by the Principal, Deputy CEO or CEO.

## 2. Data Security

Landau Forte systems store sensitive information about students, parents, carers, staff etc. Therefore, you need to ensure that when you access sensitive data you adhere to the following rules:

- Do not view sensitive information in areas where you can be overlooked, especially when in teaching rooms and whilst connected to a projector.
- Do not allow any other user to use a PC/Laptop whilst you are logged on. Everyone who is authorised to use the computer systems has their own username and password issued to them.
- Do not share information about students, staff or parents with external bodies unless this is securely transferred or part of our legal obligation (requests from exam boards or social services would be in line with legal obligations). **For advice on how to securely send information by email please seek assistance from the IT team via the IT helpdesk.**
- When you have finished using the computer system ensure that you exit the software and log off.
- Passwords should **be a minimum of at least** eight characters, with a mixture of lower and UPPERCASE letters, and include at least one number.
- Passwords should also not be used across systems, please make sure you use different passwords for each system.
- If you suspect someone knows your password contact the Systems Support Team as soon as possible, and request that your password is changed.
- The computer systems should only be used by authorised and trained staff in the furtherance of their duties at Landau Forte.

**Before using any third party applications or systems, please ensure that you are familiar with the Trust Data protection policy and legal obligations for Data Processing. Please also ensure that you have read and are familiar with the Trust guidelines on use of external applications and systems.**

### Windows Security:

- Lock your PC/Laptop if you have to leave it unattended.
- To do this, press CTRL + ALT + DEL and choose the 'Lock this computer' option.
- Ensure that your screensaver is enabled and the time delay is set for a period of no more than ten minutes.

### **Data Validity:**

- Data stored in the MIS is constantly updated, therefore any data exported from the MIS into other systems/formats should only be considered as valid for a maximum period of 1 week.
- Ensure that updated information provided by parents and carers is passed onto administration staff so that the MIS can be updated.

### **Physical Security:**

- Sensitive data stored in either electronic or printed format should be kept in a locked cabinet as it is subject to Data Protection.
- Users may not copy, remove or transmit sensitive data from Landau Forte unless the media (USB drive, External Hard Drive, CD, DVD, etc) or transfer (email, website, FTP etc) is encrypted and password protected in addition to being transported for storage in a secure location.
- Landau Forte recommends the use of the Remote Access system, details can be found on the website.
- When it is no longer needed, sensitive paper based data must be destroyed by shredding or in a confidential waste bin.
- When it is no longer needed, sensitive electronic data must be destroyed by secure overwriting.

## **3. Portable devices and other equipment**

Portable Devices and other equipment may be provided for use by you in the furtherance of your duties and responsibilities at Landau Forte such as laptops, tablets, and smartphone/phones. The equipment is on loan to you and remains the property of Landau Forte. Its use is subject at all times to compliance with this policy.

### **Security**

The device *MUST* be locked away when not in use:

#### **During the day:**

- For short periods such as breakfast or lunch, the device should be locked in a staff workroom, your teaching room or locked in a filing cabinet.
- For longer periods such as overnight, weekends or holidays, the device should be locked in a staff workroom or returned to the Systems Support Team for safe keeping.

#### **Off-Site Use:**

- If the device is taken off-site, it is your responsibility to ensure that it is covered by your own home contents or other insurance. If lost, damaged or stolen whilst away from Landau Forte, then you are responsible for the device's replacement or repair.
- Staff laptop value for insurance purposes is £500.

### **Improper Use**

Use of a portable device, like any other Landau Forte equipment, is subject to compliance with all Trust policies, in particular the Data Protection policy and safeguarding policies should also be read in conjunction with this policy.

Transfer of sensitive or personal data from Landau Forte equipment systems or premises to unauthorized personal or external parties may constitute a Data Breach.

### **Good Housekeeping**

- Ensure that portable devices are carried around in a suitable case in order to avoid any damage to the device when not in use.
- Other items should not be placed on top of the device.
- The device should not be placed face down on a surface. It should always remain face up.
- In the event of failure, when a portable device is returned to the Systems Support Team, no responsibility can be accepted for the recovery of personal data or programs.
- Do not remove any labelling or security identification markings on any Landau Forte equipment, or mark the equipment with any other labels/stickers.

**This policy should be read in conjunction with the Data Protection policy, Safeguarding Policy and other relevant academy and Trust policies. Failure to adhere to these policies could result in disciplinary action.**

**By signing to confirm that you have read and understood this policy you confirm that you understand that all Internet usage and network usage is logged and that this information can be reviewed by the Trust upon request. You also understand that failure to comply with this agreement could lead to disciplinary action.**

**Date.....**

**Signed.....**