LANDAU FORTE ACADEMY QEMS

LANDAU FORTE ACADEMY TAMWORTH SIXTH FORM

Policy Name	Online Policy
Policy Number	LFTSFQ/0013
Date of Issue	September 2023
Reviewed by	Mr N Hill
Date of next review	September 2024

(1) Introduction

Safeguarding children is defined in Working together to safeguard children https://www.gov.uk/government/publications/working-together-to-safeguard-children--2 as:

- protecting children from maltreatment
- preventing impairment of children's health or development
- ensuring that children are growing up in circumstances consistent with the provision of safe and effective care
- taking action to enable all children to have the best outcomes

All staff are required to read the following document:

- Keeping Children Safe in Education - Statutory Guidance for Schools and Colleges https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

(2) Policy Statement

2.1 This Policy applies to all members of the Landau Forte Academy Sixth Form/QEMS (including staff, volunteers, Parent/Carers, visitors and community users) who have access to and are users of Campus ICT systems, both in and out of the Campus.

2.2 Landau Forte Academy Sixth Form/QEMS recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. Despite the age group of our students, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the Campus and to support students and staff to identify and manage risks independently. Landau Forte Academy Sixth Form/QEMS believes this can be achieved through a combination of security measures, training, guidance and implementation of our associated policies. The Campus's Online Safety Policy will operate in conjunction with other policies and will comply with relevant legislation (see below).

2.3 We will not allow students to access social networking sites on Campus computers. Campus social networking sites are intended to support independent study and encourage student collaboration outside of the Campus and can therefore be accessed at home from personal devices.

2.4 We have in place Internet filtering systems to monitor and safeguard students from accessing inappropriate sites or any material of terrorist and extremist nature. This software is regularly reviewed and monitored to ensure that the filtering is appropriate and suitable for the age ranges of the students using the system. Where students accidently access inappropriate or explicit material, they should immediately report this to their Personal or Subject Tutor.

2.5 We will raise student awareness of using digital technology and ensure they are aware of how to protect themselves online through Online Safety sessions, delivered through the Tutorial Programme.

2.6 Details of those responsible for Online Safety at Landau Forte Academy Sixth Form/QEMS are shown in Appendix 1.

(3) The Internet

3.1 Students should not attempt to access or upload on the Internet information that is obscene, sexually explicit, racist, and defamatory, incites or depicts violence, or describes techniques for criminal or terrorist and extremist acts.

3.2 Students must not attempt to deliberately re-route their connection to avoid the Campus proxy server, or falsify usage logs in order to escape detection.

3.3 All teachers and students at the Campus are made aware of the risks posed by the online activity of extremist and terrorist groups through our staff training sessions and procedures they need to follow in reporting any issues involving: the Internet; use of social networking sites; email; mobile phones and other devices.

(4) Use of Social Networking Sites (including Twitter, blogs and other similar sites)

4.1 Students, staff and the wider community should be conscious at all times of the need to keep their personal and Campus lives separate. They should not put themselves in a position where there is a conflict between the Academy and their personal interests. Users should not engage in activities involving social media which might bring the Campus into disrepute; represent their personal views as those of the Campus on any social medium; discuss personal information about other students, the Campus and the wider community they interact with on any social media; use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or the Campus.

4.2 Students and members of the wider school community should not identify themselves as members of the Campus in their personal web-space, unless specifically linked to an approved job role within the Campus community where it serves a purpose to professionally market the school. This is to prevent information being linked with the Campus and to safeguard the privacy of staff members, students and Parents/Carers and the wider school community.

4.3 Students should not have contact through any personal social medium with any member of staff, whether from the Campus or any other school/college, other than those mediums approved by the Principal unless the staff concerned are family members. If students and members of the wider school community wish to communicate with staff they should only do so through official school sites created for this purpose, which at present are Campus website, Campus email and the VLE.

4.4 Information that students and members of the wider community have access to as part of their involvement with the Campus, including personal information, should not be discussed on their personal web space.

4.5 We advise that Campus email addresses should not be used for setting up personal social media accounts or to communicate through such media.

4.6 All staff, Parents/Carers, students and members of the wider community are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. All staff, Parents/Carers, students and members of the wider community should keep their passwords confidential, change them often and be careful about what is posted online.

4.7 The Campus accepts that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. Linkedin. The Campus would advise that care is taken to maintain an up to date profile and a high level of presentation on such sites if the Campus is listed.

Guidelines for safe Social Media usage can be found on the following websites:

http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

http://www.childline.org.uk/explore/onlinesafety/pages/socialnetworking.aspx

http://www.getsafeonline.org/social-networking/social-networking-sites/#.Uq7_0lPs084

http://www.bbc.co.uk/webwise/courses/social-media-basics/lessons/stay-safe-on-social-networks

4.8 Where social media sites are to be used for educational purposes, a Risk Assessment should be carried out to determine which tools are appropriate. All social media services must be approved by the Director of Sixth Form/Head of School. Staff will be given the Campus's 'Guidelines for creating and maintaining social media accounts' document. In addition, a signature will be required in advance of any work being undertaken

4.9 See Appendix 2 'Guidelines for creating and maintaining social media accounts'

(5) Email

5.1 Staff and students should only use e-mail addresses that have been issued by the Campus and the e-mail system should only be used for Campus-related matters. Students and staff are advised to maintain an alternative personal e-mail address for use at home in non-Campus related matters.

5.2 Staff should not contact Parent/Carers via email without prior consultation with the Principal.

5.3 Downloading and passing on copyright information or material which may be considered to incite hatred, or pose risks by the material of extremist and terrorist groups will be treated by the Campus as gross misconduct. Be aware that such material which may be contained in jokes sent by email can be considered to be harassment. Any person receiving such email should report it to a member of staff.

5.4 Users must not knowingly send or receive information that will bring the Campus into disrepute.

5.5 Information sent by email may become subject to the Data Protection Act and this must be complied with where appropriate. Students should not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

(6) Mobile Phones and other devices

6.1 As a general presumption and as a matter of courtesy, all mobile phones (students and staff) should be switched off whilst in lessons. However, there may be times when some of the features of mobile phones may be beneficial to the learning activities in a lesson (e.g. students may wish to capture photographs/videos of an experiment). In such cases, mobile devices can be used, once permission has been granted by the Tutor. No images should be taken of staff or students without their permission.

6.2 If a member of staff suspects that a mobile phone has been misused (extreme, poses risks to the students from terrorist and extremist material) within the Campus, it should be confiscated, but staff should not 'search' the phone. The incident should be passed directly to the Senior Leadership Team who will deal with the matter in line with normal Campus procedures.

6.3 Students should report any instances of unwanted or distressing text messages to their Tutor or relevant member of staff.

6.4 The Campus will work with the student to report to the Police if necessary. Students should never forward explicit or embarrassing texts or images if they receive them, as it is illegal to send explicit images to other young people. This is also the case for any material of terrorist/extremist nature, as we ensure that students are safe and are not exposed to such material.

6.5 Students should consider the content before sending images or information about other people. Never give out anyone else's number or take a photograph of them without their agreement.

6.6 Students who are uncomfortable about any pictures or messages that have been sent to them will be encouraged to keep a record of them as they could be used as evidence. Their network operator may be able to help against nuisance calls. Student can also speak to their Tutor.

(7) Publish Student's Images and Work

7.1 Students are asked for their consent to allow photographs and videos that may be taken of them to be used for Campus promotional purposes for example in leaflets and online. This is recorded, held centrally and is available to staff who need to ensure that images are not used without consent.

7.2 If students do not wish to have their photographs taken, they can opt out and this choice should be communicated with the students.

7.3 Work can only be published with the written permission of the student.

(8) Use of Photographs and Video

8.1 The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from Parent/Carers be gained if videos or photographs of students are going to be used.

8.2 Photographs, videos or any other types of image of students and their families or images depicting staff members, clothing with Campus logos or images identifying school premises should not be published on personal or public web space without prior permission from the Campus. Students and the wider school community should not post images or videos from Campus events on any public social media site. Images or videos taken at school events, when such permission has been granted by the Campus, are for the sole and private use of that individual and their use must be in accordance with the Data Protection Act 1998.

8.3 Staff must be fully aware of the consent form responses from Parent/Carers when considering use of images.

8.4 Staff should always use a Campus camera to capture images and should not use their personal devices.

8.5 Photographs taken by the Campus are subject to the Data Protection Act.

(9) Photographs and Videos taken by Parents/Carers

9.1 Parents/Carers are permitted to take photographs/videos of their own children in Campus events. However, they are requested not to share photographs/videos from Campus events on social networking sites if other students appear in the background.

9.2 A Parent/Carer letter regarding the Acceptable Use Agreement (AUA) should include a paragraph concerning posting photographs/videos on social networking sites. Photographs for personal use such as those taken by Parents/Carers are not subject to the Data Protection Act.

(10) Internet Use and Acceptable User Agreement (AUA)

10.1 Landau Forte Academy Sixth Form/QEMS is committed to preventing people from being drawn into terrorism. There is a filtering system in place to restrict access (by staff and students) to harmful content online. If staff need to access material for educational purposes which is blocked by the filtering system, then a request should be sent to the IT Support team support@lfatq.org.uk. If there are any queries, the System Manager can discuss these where required. If students need to access material for education purposes, this should be discussed with their tutor who can refer this to IT Support where appropriate. There will be a central list of websites, which staff and students have asked to be unblocked, and reasons for this. The Safeguarding Team will monitor this list. Landau Forte Academy Sixth Form/QEMS reserve the right to monitor all online activity through the server and to take action if the content is deemed to be inappropriate.

(11) Dealing with Bullying issues

11.1 The Campus's Online Safety Policy and/or Anti-bullying Policy should make clear the sanctions regarding bullying using new technologies.

11.2 The Campus can take action against incidents that happen outside Campus if it could have repercussions for the orderly running of the Campus or poses a threat to another student or member of the public or could adversely affect the reputation of the Campus.

11.3 Use of social networking sites to harass, bully or intimidate would be covered by this irrespective of when/where the post was made.

(12) Reporting

12.1 All breaches of the Online Safety Policy need to be recorded including details of the user, date and incident. Incidents which may lead to safeguarding issues need to be passed on immediately to the member of the Senior Leadership Team responsible for Online Safety – it is their responsibility to decide on appropriate action not the Tutor. Incidents which are not safeguarding issues but may require Senior Leadership Team intervention (e.g. cyberbullying) should be reported to the Senior Leadership Team on the same day.

12.2 Allegations involving staff should be reported to the Principal. If the allegation is one of abuse, it should be handled according to the DfE document entitled 'Dealing with allegations of abuse against teachers and other staff'. Evidence of incidents must be preserved and retained.

12.3 Please refer to Appendix 3 for the 'Procedure for Reporting Online Safety Incidents'.

(13) Breaches of this Policy

13.1 Any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of the Campus or any illegal acts or acts that render the Campus liable to third parties may result in legal action, disciplinary action or sanctions in line with the published Campus policies for staff and students.

(14) Handling Online Safety Complaints

14.1 Complaints of Internet misuse will be dealt with by a member of Senior Leadership Team.

14.2 Complaints concerning safeguarding issues will be dealt with according to the Campus Safeguarding Policy.

14.3 Students and Parents/Carers will be informed of the complaints procedure.

(15) Relevant Legislation

15.1 Data Protection Act 1998

15.1.1 A Campus, like every other data user, must conform to the requirements of the Data Protection Act (1998). In particular this requires the Campus to formally notify the Information Commissioner of:

- the purposes for which the school holds personal data;
- what data it holds;
- the source of the data;
- to whom the data is disclosed.

15.1.2 Under the Act, each Campus is a separate data user and must complete a “Notification” each year.

15.1.3 It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

15.2 Computer Misuse Act 1990

15.2.1 Under the Computer Misuse Act 1990, the following are criminal offences if undertaken intentionally:

- Unauthorised access to a computer system or data
- Unauthorised access preparatory to another criminal action
- Unauthorised modification of a computer system of data

15.3 Copyright, Designs and Patents Act 1988

15.3.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of ‘literary work’ covers computer programs and data.

15.3.2 Where computer programs and data are obtained from an external source, they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

15.3.3 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective license or contract.

15.3.4 The Campus is responsible for compiling and maintaining an inventory of all software held, including freeware and shareware, and for checking it at least annually to ensure that software licenses accord with installations. To ensure that the Campus complies with the Copyright, Designs and Patents Act 1988, users must get prior permission in writing from their SIRO (or nominated person) before copying any software.

15.3.5 Freeware or shareware software should be registered as required with the software supplier and is generally provided on an unsupported basis. The

Campus need to be extremely cautious in accepting free downloadable software over the internet. Very often free software also loads malware software onto the PC. Malware resides and hides on computers, often reporting back to advertising companies or other data capture firms that build up a profile of internet browsing habits.

15.3.6 Users should read all licence agreements very carefully before accepting the terms and conditions and, if in any doubt, should not accept the licence conditions/download.

15.3.7 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of Campus policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

15.4 Freedom of Information

15.4.1 The Freedom of Information Act (FOI) came into force on 1st January 2005. This means that members of the public and organisations have rights of access to information held by public bodies. Upon request we must tell individuals if we hold information and if so, provide it within 20 working days.

15.4.2 The principle behind the Act is that all information held in any format is accessible, unless certain conditions or exemptions apply.

15.5 Human Rights

15.5.1 The Campus must act in a way that is compatible with and promotes individuals' rights in accordance with the Human Rights Act 1998.

15.5.2 Definitions of Personal Information and Sensitive Personal Information for this purpose are:

15.5.2.1 Personal data - information that is sufficient to identify a living individual by itself or in conjunction with other information held by the Academy. Includes any expression of opinion about an individual and any indication of the intentions of the Academy or any other person in respect of the individual

15.5.2.2 Sensitive personal data - defined in the Data Protection Act 1998 as information about an individual relating to physical/mental health, criminal proceedings, ethnicity, sexual life, trade union, political opinions or religious beliefs

15.5.2.3 Other data - that should be protected includes: national insurance number, bank account details, credit card details, identification credentials and protected whereabouts

(16) Handling Online Safety Complaints

16.1 The Campus does not currently support student devices on the Campus wireless network.

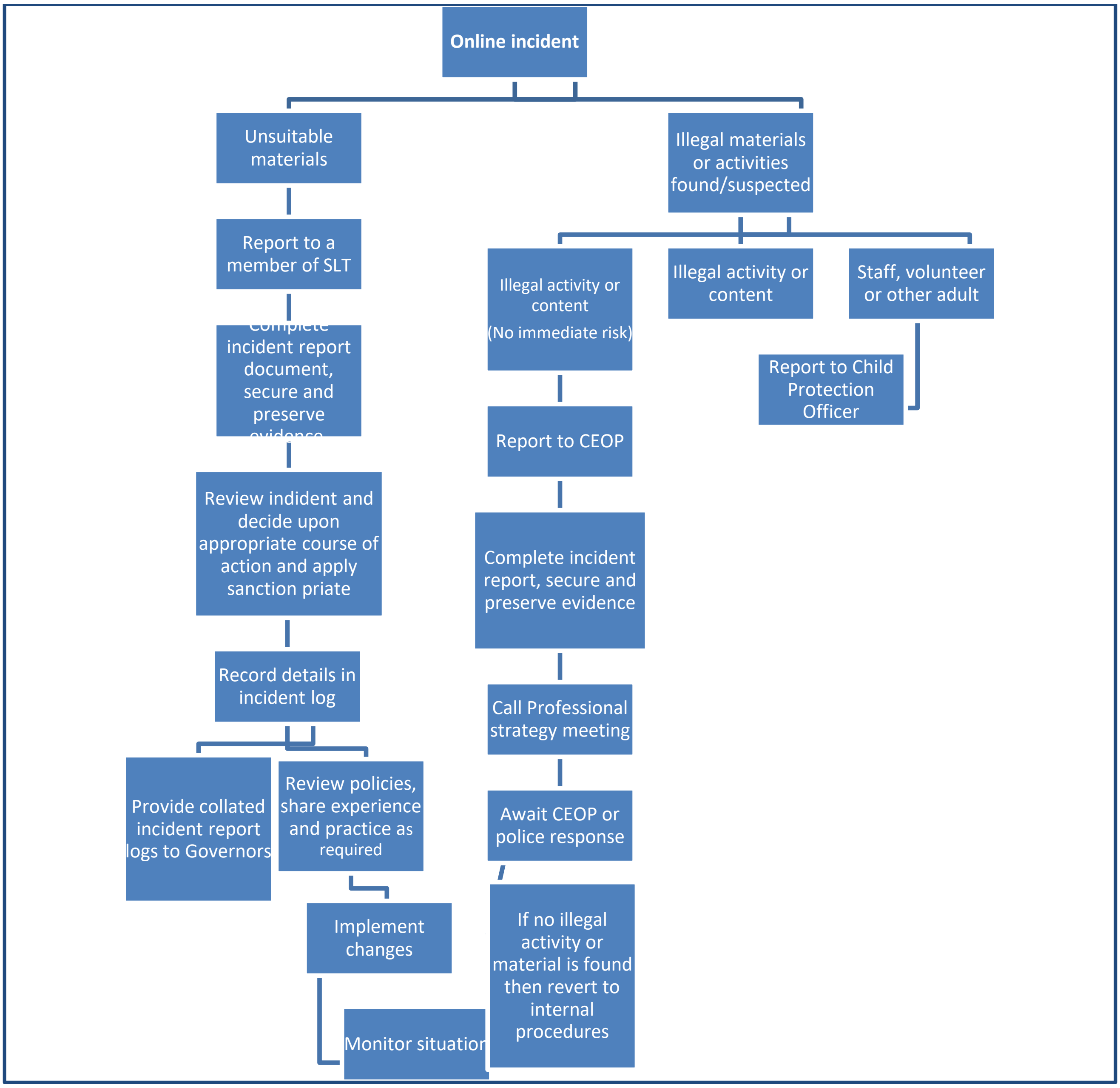
(17) Related Documents

- Campus Policy 0001 Safeguarding incorporating Child Protection
- Campus Policy 0074 Behaviour Policy
- Campus Policy 0014 Bullying and Discriminative Behaviours
- Campus Policy 0047 Data Protection Policy

Appendix I
Responsibilities for Online Safety

Role	Name	Job Title
Member of Senior Leadership Team responsible for Online Safety	Mr N Hill	Designated Safeguarding And Mental Health Lead
Online Safety Co-ordinator	Mrs C Wright	Deputy Safeguarding and Mental Health Lead
Governor responsible for Online Safety	Mrs K Tromans	Governor

Appendix 2
Procedure for reporting Online Safety Incidents


Online incident
Unsuitable materials
Report to a member of SLT
Complete incident report document, secure and preserve evidence
Review indident and decide upon appropriate course of action and apply sanction priate
Record details in incident log
Provide collated incident report logs to Governors
Review policies, share experience and practice as required
Implement changes
Monitor situation
Illegal materials or activities found/suspected
Illegal activity or content
(No immediate risk)
Report to CEOP
Complete incident report, secure and preserve evidence
Call Professional strategy meeting
Await CEOP or police response
If no illegal activity or material is found then revert to internal procedures
Illegal activity or content
Staff, volunteer or other adult
Report to Child Protection Officer

Appendix 3
Guidelines for creating/maintaining staff campus social media accounts

When creating social media accounts staff are required to adhere to the following:

1. Administrator email addresses should be email accounts provided by the Campus and not personal email accounts
2. Passwords should be minimum of 10-12 characters in length, not in use elsewhere and changed immediately if you think they are compromised
3. Usernames and passwords should be held by more than one member of a department/faculty.

When maintaining social media accounts staff are required to abide by the following:

4. Social media services must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages
5. Social media services must not be used for the promotion of personal financial interest, commercial ventures or personal campaigns
6. Social media services must not be used for actions that would put staff in breach of the Campus's codes of conduct or policies
7. Social media services must not breach the Campus's equality and diversity policies
8. Staff should not use the account to enter into direct communication with students that would breach 'Guidance for safer working practice for adults who work with children and young people'
9. The social media site should be used purely for educational purposes and not personal purposes
10. Photographs of students should not be posted unless permission has been gained from Parent/Carer
11. Full surnames of students should never be published

Before promoting the use of social media sites as a tool for independent learning and student collaboration off site, the following information and guidance delivered through the Pastoral Programme must be reinforced:

12. Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications when using social networking sites
13. Students should be encouraged to ensure that virtual communications areas are open only to known friends
14. Students should be encouraged to report any instances of online bullying to a member of staff. Any student found guilty of using online systems for bullying or harassment of other students will be subject to the Campus disciplinary procedure
15. Students should be reminded that individuals that they meet online may not be trustworthy. People are not always what they first might appear
16. Adults who go online to chat to young people and arrange to meet in order to have sex are breaking the law. Students will be encouraged to report any instance of online activity that makes them feel uncomfortable to a member of staff
17. Students should be aware of the effects of online activities which includes illegally downloading media, as well as bullying others. They are not anonymous online and activity will be monitored both inside and outside the Campus.

Appendix 4
Staff Acceptable Use Agreement for ICT Systems (AUA)

I understand that I must use Campus ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the Campus will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Campus ICT systems (e.g. laptops, email, VLE etc.) out of Campus and to the transfer of personal data (digital or paper based) outside of the Campus.
- I understand that the Campus ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Campus
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I should not write down or store my password. I will choose a suitably strong password for Campus systems and not reuse the same password for all of my accounts.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Director of the Sixth Form.

I will be professional in my communications and actions when using Campus ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Campus's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the Campus website, VLE etc.) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in the Campus in accordance with the Campus's Online Safety Policy
- I will only communicate with students using official Campus systems (Campus email system, VLE etc). Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not request or accept friend requests from current students on any social network.

The Campus has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Campus:

- When I use my mobile devices (laptops / mobile phones / USB devices etc.) in the Campus, I will follow the rules set out in this agreement, in the same way as if I was using Campus equipment. I will also follow any additional rules set by the Campus about such use. I will ensure that any such devices are password protected and appropriate care taken with regards to security.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs). In the event of any concern regarding an email or attachment, do not forward any suspect email; IT Support can help and advice if you have any concerns.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse ages, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering /security systems in place to prevent access to such materials.
- Landau Forte Sixth Form/QEMS is committed to preventing people from being drawn into terrorism. There is a filtering system in place to restrict access (by staff and students) to harmful content online. If staff need to access material for educational purposes which is blocked by the filtering system, then a request should be sent to the IT Support team support@lfatq.org.uk. If there are any queries, the System Manager can discuss these where required. If students need to access material for education purposes, this should be discussed with their tutor who can refer this to IT Support where appropriate.

Appendix 4
Staff Acceptable Use Agreement for ICT Systems (AUA)

- There will be a central list of websites, which staff and students have asked to be unblocked, and reasons for this. The Safeguarding Team will monitor this list. Landau Forte Sixth Form/QEMS reserve the right to monitor all online activity through the server and to take action if the content is deemed to be inappropriate
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to Campus equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Campus policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Campus sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the Campus:

- I understand that this Acceptable Use Agreement applies not only to my work and use of the Campus ICT equipment in Campus, but also applies to my use of ACampus ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Campus
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.
- I understand that I should not have contact through any personal social medium with students, whether from the Campus or any other school/college, other than those mediums approved by the Principal unless the staff concerned are family members. If I wish to communicate with students, I will do so through official school sites created for this purpose which, at present, are the Campus email and the VLE.
- I understand that I should not engage in activities involving social media which might bring the Campus into disrepute.
- I understand that I am not to represent my personal views as those of the Campus on any social network.
- I understand that I should not discuss personal information about students, the Campus and the wider community I interact with on any social network
- I understand that I should not use social media and the internet in any way to attach, insult, abuse or defame students, their family members, members of staff, other professional, other organisation or the Campus.

I understand that any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of the Campus or any illegal acts or acts that render the Campus liable to third parties may result in legal action, disciplinary action or sanctions in line with the publish Campus policies for students. I have read and understand the Online Safety Policy and the above. I agree to use the Campus ICT systems (both in and out of Campus) and my own devices (in Campus and when carrying out communications related to the Campus) within these guidelines.

Each member of staff is required to sign to acknowledge having read and understood this Agreement

Staff Name	
Signature	
Date	

Appendix 5
Student Acceptable Use Agreement for ICT Systems (AUA)

All students must use the Campus ICT systems in a responsible way to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. Students should adhere to the guidelines detailed below.

For a student's personal safety:

- The Campus will monitor the student's use of the systems, devices and digital communications, including all files stored anywhere on the Campus network, student internet activity and emails sent/received
- The student should keep their username and password safe and secure and not share this information, nor should they try to use any other person's username and password. They should not write down or store a password where it is possible that someone may steal it
- The student should not leave their login session unattended
- All use of an account is the responsibility of the student to whom the account is allocated to, and any suspected misuse should be reported to a Tutor immediately
- The student should be aware of 'strangers' when communicating online
- The student should not disclose or share personal information about themselves or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- The student should immediately report to the Safeguarding Team any unpleasant or inappropriate material or messages or anything that makes them feel uncomfortable when seeing it online

The student should understand that everyone has equal rights to use technology as a resource and:

- That the Campus systems and devices are primarily intended for educational use and not use them for personal or recreational use unless appropriate permission has been granted
- Should not try (unless appropriate permission has been granted) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- Should not use the Campus systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube)

The student should act as they expect others to act towards them and:

- Respect others' work and property and not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
- Be polite and responsible when communicating with others, not use strong, aggressive or inappropriate language and appreciate that others may have different opinions
- Not take or distribute images of anyone without their permission

The student should recognise that the Campus has a responsibility to maintain the security and integrity of the technology it offers them and, to ensure the smooth running of the Campus, the student should:

- Only use their own personal devices (mobile phones, USB devices etc.) in the Campus if they have been granted permission and should understand that, if they do use their own devices in the Campus, they should follow the rules set out in this agreement in the same way as if they were using Campus equipment
- Understand the risks and not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor should they use any programs or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials
- Immediately report any damage or faults involving equipment or software, however this may have happened
- Not open any hyperlinks in emails or any attachments to emails, unless they know and trust the person/organisation who sent the email or if they have any concerns about the validity of an email (due to the risk of the attachment containing viruses or other harmful programs)
- Not install or attempt to install or store programs of any type on any school device, nor try to alter computer settings

Appendix 5
Student Acceptable Use Agreement for ICT Systems (AUA)

When using the internet for research or recreation, the student should:

- Ensure they have permission to use the original work of others in their own work
- Where work is protected by copyright, not try to download copies (including music and videos)
- When using the internet to find information, take care to check that the information accessed is accurate, understanding that the work of others may not be truthful and may be a deliberate attempt to mislead them

The student is responsible for his/her actions, both in and out of the Campus and should not:

- Have contact through any personal social media with any member of staff, whether from the Campus or any other school/college, other than those mediums approved by the Principal, unless the staff concerned are family members. If students wish to communicate with staff, they should do so through official school sites created for this purpose, which at present are the Campus website and Campus email.
- Engage in activities involving any social media which might bring the Campus into disrepute
- Represent their personal views as those of the Campus on any social media
- Discuss personal information about other students, the Campus and the wider community on any social media
- Use social media and the internet in any way to attack, insult, abuse or defame students, their family members, Campus staff, other professionals, other organisations or the Campus.

The student agrees to follow these guidelines when using:

- The Campus systems and devices (both in and out of the Campus)
- Their own devices in the Campus (when permission is granted) e.g.mobile phones, cameras etc
- Their own equipment out of the Campus in a way that is related to them being a member of the Campus e.g. communication with their peers and members of staff, accessing Campus email, communicating on Campus Twitter pages etc.

The student understands that:

- Any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of the Campus or any illegal acts or acts that render the Campus liable to third parties may result in legal action, disciplinary action or sanctions in line with the published Campus policies for students
- Should the student be found to have caused damage to any equipment, s/he will be liable to sanctions.

Each student is required to sign to acknowledge having read and understood this Agreement

Student Name	
Signature	
Date	

Date	**September 2023**
Change Made	**Various**
Made By	**Mr N Hill**