Policy Name	**Online Safety Policy**
Policy Number	**LFTSFQ/0013**
Date of Issue	**September 2026**
Reviewed by	**Mrs C Wright**
Date of next review	**September 2027**

(1) Purpose

Landau Forte QEMS recognises that technology plays an important role in education, communication and everyday life. The school is committed to ensuring that all members of our community can use digital technology safely, responsibly and positively.

This Online Safety Policy sets out the expectations for the safe and appropriate use of the internet, computers, tablets, mobile phones, social media, online learning platforms, email, gaming platforms and other digital services.

The school takes guidance from Keeping children safe in education 2026.

The policy aims to:

- Protect pupils, staff and visitors from online risks and harm.
- Promote responsible, respectful and safe use of technology.
- Teach pupils how to identify and respond to online risks.
- Prevent inappropriate access to or sharing of harmful, illegal or unsuitable material.
- Reduce the risk of cyberbullying, online abuse, grooming, exploitation and other forms of digital harm.
- Protect personal information, school data and digital accounts.
- Provide clear procedures for reporting and responding to online safety concerns.
- Support parents and carers in helping children stay safe online.

(2) Policy Scope

This policy applies whenever members of the Landau Forte QEMS community are using:

- School computers, laptops, tablets and other devices.
- School Wi-Fi and network systems.
- School email accounts.
- Online learning and communication platforms.
- School-managed cloud storage and applications.
- Personal devices when they are connected to school systems.
- Social media, messaging services and online platforms where behaviour may affect the safety, wellbeing or reputation of members of the school community.

The school's expectations may also apply to online behaviour outside school where it has an impact on pupils, staff, the school community or safeguarding.

(3) Policy Statement

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.

Landau Forte Academy Sixth Form/QEMS 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).

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.

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.

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.

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

(4) Roles and Responsibilities

The Governing Body

The Governing Body will:

- Ensure that appropriate online safety arrangements are in place.
- Support the school in meeting its safeguarding responsibilities.
- Ensure that online safety is reviewed regularly.
- Ensure that staff receive appropriate training.
- Monitor the effectiveness of the school's online safety arrangements.

Senior Leadership Team

The Senior Leadership Team will:

- Promote a culture of safe and responsible technology use.
- Ensure that online safety forms part of the school's safeguarding arrangements.
- Ensure concerns are appropriately investigated and recorded.
- Work with the Designated Safeguarding Lead and other relevant staff when concerns arise.
- Ensure appropriate action is taken when this policy is breached.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) will:

- Coordinate responses to online safeguarding concerns.
- Ensure online safety concerns are recorded and followed up appropriately.
- Liaise with parents/carers and external agencies where necessary.
- Ensure staff understand how online activity may form part of wider safeguarding concerns.
- Ensure relevant safeguarding information is shared appropriately.

Staff

All staff are expected to:

- Follow this policy and the school's Acceptable Use Agreement.
- Model safe, respectful and professional online behaviour.
- Keep passwords and accounts secure.
- Use school-approved systems and platforms wherever possible.
- Report safeguarding, cyberbullying, inappropriate content or other online safety concerns promptly.
- Maintain appropriate professional boundaries with pupils online.
- Avoid using personal accounts to communicate privately with pupils.
- Complete required online safety training.

Pupils

Pupils are expected to:

- Use technology responsibly and respectfully.
- Follow the school's Acceptable Use Agreement.
- Protect their passwords and account information.
- Never attempt to access another person's account.
- Report harmful, inappropriate or suspicious online activity.
- Never share another person's personal information, images or videos without permission.
- Treat others with respect online and offline.
- Follow age restrictions and school rules relating to online services.
- Understand that online actions can have consequences.

Parents and Carers

Parents and carers are encouraged to:

- Discuss online safety regularly with their children.
- Monitor age-appropriate online activity.
- Encourage children to report anything that makes them feel uncomfortable, frightened or unsafe.
- Use parental controls where appropriate.
- Inform the school of significant online concerns affecting their child.
- Support the school's expectations regarding responsible use of technology.

(5) Acceptable Use of Technology

All users of school technology must use digital systems appropriately.

Users must:

- Use technology primarily for authorised educational or work-related purposes.
- Follow instructions from staff.
- Keep usernames and passwords confidential.
- Lock or log out of devices when they are not being used.
- Take reasonable care of school equipment.
- Only access files, systems and information they are authorised to use.
- Respect copyright and intellectual property.
- Communicate politely and respectfully.

Users must not:

- Attempt to bypass school filtering, monitoring or security systems.
- Access or distribute illegal, offensive, discriminatory or inappropriate material.

- Use another person's account or impersonate another person.
- Share passwords or authentication information.
- Deliberately damage school devices or systems.
- Install unauthorised software or applications.
- Use school systems to bully, threaten, harass or intimidate others.
- Record, photograph or film others without appropriate permission.
- Use technology to commit or encourage illegal activity.

(6) Internet Filtering and Monitoring

Landau Forte QEMS will use appropriate technical measures to help protect users from harmful or inappropriate online content.

These measures may include:

- Web filtering.
- Network security.
- Device management.
- Anti-virus and security software.
- Monitoring of school-managed accounts and systems.
- Blocking or restricting access to inappropriate websites, applications or services.

Filtering and monitoring are important safeguarding measures but cannot remove every online risk. The school will therefore combine technical protection with education, supervision and clear reporting procedures.

Where monitoring identifies a safeguarding concern, the matter may be referred to the DSL or another appropriate member of staff.

(7) The Internet

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.
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.

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.

(8) Personal Data and Privacy

All members of the school community must protect personal information.

Personal information must not be:

- Shared with unauthorised individuals.
- Posted publicly without appropriate permission.
- Stored on unauthorised devices or services.
- Sent through insecure or inappropriate channels.
-

Staff must follow the school's Data Protection and Privacy procedures and relevant data protection legislation.

Pupils will be taught to understand the importance of protecting information such as:

- Full name.
- Address.
- Telephone number.
- Passwords.
- School information.
- Location.
- Photographs and videos.
- Personal or family information.

(9) Passwords and Account Security

Users must take responsibility for keeping their accounts secure.

Passwords should:

- Be kept confidential.
- Not be shared with friends or colleagues.
- Be difficult for others to guess.
- Not be reused unnecessarily across different services.

If a user believes that their account or password has been compromised, they must report this immediately and change the password where appropriate.

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

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.

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.

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.

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.

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

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

The Campus accepts that some sites may be used for professional purposes to highlight a personal profile with 7ummarized 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

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

(11) Email

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.

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.

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

(12) Cyberbullying and Online Abuse

Cyberbullying includes bullying or harassment using digital technology, including social media, messaging applications, gaming platforms, email and other online services.

Examples include:

- Threatening or abusive messages.
- Deliberately excluding someone from online groups.
- Spreading rumours.
- Sharing embarrassing photographs or videos.
- Creating fake accounts to impersonate someone.
- Posting hateful or discriminatory comments.
- Encouraging others to target an individual.
- Sharing private information without permission.

Landau Forte QEMS will not tolerate cyberbullying.

Any pupil who experiences or witnesses cyberbullying should:

1. Avoid responding to abusive messages where possible.
2. Save evidence, such as screenshots or messages.
3. Block or report the account where appropriate.
4. Tell a trusted adult.
5. Report the matter to the school where it involves members of the school community.

The school will investigate concerns and take appropriate action in accordance with its behaviour, safeguarding and disciplinary procedures.

(13) Social Media

Pupils should understand that information posted online can be copied, shared and remain accessible for a long time.

Pupils must not use social media to:

- Bully or threaten others.
- Share private or confidential information.
- Post discriminatory or hateful content.
- Share inappropriate photographs or videos of other pupils or staff.
- Damage the reputation of individuals or the school.
- Encourage dangerous, illegal or harmful behaviour.

Staff must maintain professional boundaries and must not communicate with pupils through personal social media accounts.

Staff should consider the potential impact of online activity on their professional role and the reputation of the school.

(14) Mobile Phones and other devices

The use of mobile phones and personal devices on school premises must follow the school's current behaviour and mobile phone rules.

Where devices are permitted, pupils must:

- Use them only at authorised times and in authorised locations.
- Follow staff instructions.
- Not use devices to photograph, film or record others without permission.
- Not use devices to access inappropriate content.
- Not use devices to bully, threaten or harass others.

The school may take appropriate action where a personal device is used in a way that breaches school rules or creates a safeguarding concern.

(15) Publish Student's Images and Work

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.

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

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

(16) Use of Photographs and Video

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.

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.

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

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

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

Please see our Taking, Storing and Sharing Students Photographs Policy

(17) Photographs and Videos taken by Parents/Carers

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.

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.

(18) Artificial Intelligence (AI)

The school recognises that artificial intelligence tools can provide valuable educational opportunities but also present risks.

Pupils must use AI tools responsibly and in accordance with teacher instructions.

Pupils must not:

- Submit AI-generated work as their own where this is not permitted.
- Use AI to facilitate cheating or academic dishonesty.
- Enter confidential or personal information into AI systems.
- Use AI to create harmful, abusive, threatening or discriminatory content.

- Create fake or misleading images, videos or recordings of others.
- Use AI to impersonate another person or cause harm.

Staff should use school-approved AI tools and follow school guidance relating to data protection, safeguarding, copyright and professional responsibilities.

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

At Landau Forte 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.

(20) Dealing with Bullying issues

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

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

(21) Online Gaming

Online gaming can provide opportunities for social interaction but may expose young people to risks including inappropriate language, contact with strangers, financial scams and harmful content.

Pupils are encouraged to:

- Use appropriate privacy settings.
- Avoid sharing personal information.
- Use strong passwords.
- Report inappropriate behaviour.
- Block users who behave inappropriately.
- Tell a trusted adult if they feel unsafe.

Parents and carers are encouraged to check the age ratings and privacy settings of games and to discuss online communication with their children.

(22) Online Grooming and Exploitation

The school recognises that offenders may use online platforms to build relationships with children and young people.

Warning signs may include:

- An online contact asking a child to keep conversations secret.
- Requests for photographs or personal information.
- Attempts to move conversations to private platforms.

- Offers of gifts, money or other incentives.
- Pressure to meet someone in person.
- Sexual or inappropriate conversations.
- Threats or blackmail.

Any concern that a pupil may be experiencing grooming or exploitation must be reported immediately to a trusted adult or the DSL.

The school will follow its safeguarding procedures and contact appropriate external agencies where necessary.

(23) Sexting and Sharing Intimate Images

The school recognises that children and young people may be pressured into creating or sharing intimate images.

Pupils should understand that:

- They should never feel pressured to create or share an intimate image.
- An image can be copied and redistributed beyond their control.
- They should not forward or save someone else's intimate image.
- They should tell a trusted adult if they receive an inappropriate image.

Staff must follow the school's safeguarding procedures when dealing with concerns involving sexual images of children and young people. Staff must not copy, save or distribute such images.

(24) Online Scams, Phishing and Fraud

Users should be cautious when receiving unexpected emails, messages, links or requests for information.

Users should:

- Check the sender before responding.
- Avoid clicking suspicious links.
- Never provide passwords or security information in response to an unexpected request.
- Report suspicious messages to the appropriate member of staff or IT support.
- Be particularly cautious of messages creating a sense of urgency or threatening consequences.

(25) Online Learning and Communication

School-approved online platforms should be used for educational communication.

Staff and pupils should:

- Use appropriate language.
- Maintain professional and respectful communication.
- Follow school rules regarding online lessons and discussions.
- Avoid sharing meeting links or access codes with unauthorised individuals.
- Not record online lessons unless authorised.
- Protect personal information.

(26) Online Safety Education

Online safety education will form part of the school's wider curriculum and safeguarding programme.

Pupils will be taught about issues including:

- Cyberbullying.
- Privacy and personal information.
- Password security.
- Online relationships.
- Grooming and exploitation.
- Sexting and image sharing.
- Social media.
- Online scams and fraud.
- Digital footprints and online reputation.
- Misinformation and disinformation.
- Artificial intelligence.
- Healthy and responsible technology use.
- How and where to report concerns.

Online safety education will be age-appropriate and responsive to emerging risks.

(27) Reporting Online Safety Concerns

Everyone has a responsibility to report online safety concerns.

Concerns can be reported to:

- A trusted member of staff.
- The Designated Safeguarding Lead.
- A form tutor or pastoral team.
- A parent or carer.
- The school's established safeguarding reporting system.

If a pupil is in immediate danger, they should seek help from a trusted adult immediately or contact the emergency services where appropriate.

Reports will be treated seriously and handled in accordance with safeguarding, behaviour and disciplinary procedures.

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

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

(28) Responding to Incidents

When an online safety incident is reported, the school will:

1. Assess the immediate risk to the individual or wider school community.

2. Provide appropriate support to those affected.
3. Record the concern appropriately.
4. Involve the DSL where safeguarding is relevant.
5. Preserve relevant evidence where appropriate.
6. Investigate the incident fairly and proportionately.
7. Contact parents/carers where appropriate.
8. Involve external agencies where necessary.
9. Apply appropriate school sanctions where school rules have been breached.
10. Review the incident to identify any lessons or preventative action.

(29) Breaches of this Policy

Failure to follow this policy may result in action under the school's behaviour, disciplinary or safeguarding procedures.

Possible consequences may include:

- Removal or restriction of access to school technology.
- Educational or restorative action.
- Behaviour sanctions.
- Parental/carer involvement.
- Disciplinary action for staff.
- Referral to external agencies where appropriate.

Serious incidents involving illegal activity, threats, exploitation, abuse or significant safeguarding concerns may be referred to the police or other relevant agencies.

(30) Handling Online Safety Complaints

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

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

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

(31) Supporting Wellbeing and Healthy Technology Use

Online safety is not only about preventing harm. The school will also promote positive digital wellbeing.

Pupils will be encouraged to:

- Take regular breaks from screens.
- Maintain a healthy balance between online and offline activities.
- Speak to someone if online activity is affecting their wellbeing.
- Recognise when online content or communication is making them anxious or distressed.
- Respect other people's boundaries online.
- Use technology in ways that support learning and positive relationships.

(32) Review of the Policy

This policy will be reviewed at least annually and whenever there are significant changes to:

- Legislation or statutory guidance.
- Online safety risks.
- School technology or systems.
- National safeguarding expectations.

- Relevant school policies or procedures.

Feedback from pupils, staff, parents/carers and governors may be considered as part of the review process.

(33) Related Policies

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy.
- Behaviour Policy.
- Anti-Bullying Policy.
- Acceptable Use Agreement.
- Data Protection and Privacy Policy.
- Staff Code of Conduct.
- Mobile Phone Policy.
- Complaints Policy.
- Whistleblowing Policy.

(34) Pupil Online Safety Statement

At Landau Forte QEMS, we expect every pupil to remember:

Be kind. Be careful. Be responsible.

If something online makes you feel uncomfortable, worried or unsafe:

STOP – don't respond.
SAVE – keep evidence if it is safe to do so.
BLOCK – block the person or account where appropriate.
REPORT – tell a trusted adult or report it to the school.

Appendix I

Responsibilities for Online Safety

Role	Name	Job Title
Member of Senior Leadership Team responsible for Online Safety	Mr A Perry	Head of School
Designated Safeguarding Lead	Mrs C Wright	Safeguarding and Mental Health Lead

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	

LANDAU FORTE CHARITABLE TRUST

Date	**September 2026**
Change Made	**Various**
Made By	**Mrs C Wright**