



Policy Name	Online Safety Policy (Including Artificial Intelligence)
Date of Issue	September 2025
Policy Number	LFTSFQ/0013
Reviewed by	Miss C Wright
Date of next review	September 2026

(1) Introduction

Landau Forte QEMS and Sixth Form is committed to ensuring that all members of the school community are safe, responsible and educated users of digital technologies, including emerging technologies such as Artificial Intelligence (AI)

Online safety is a core safeguarding responsibility and forms part of the school's statutory duties under Keeping Children Safe in Education (KCSIE 2025) and the Online Safety Act. This policy applies to all students, staff, governors, volunteers, contractors and visitors.

The aims of this policy are to:

- Protect students from harmful, inappropriate, misleading or illegal content
- Promote safe, ethical and critical use of AI and digital technologies
- Ensure effective filtering, monitoring and reporting systems
- Embed online safety education across the curriculum, including misinformation and AI Literacy
- Provide clear procedures for managing online safety incidents and safeguarding concerns

Scope

This policy applies to

- All use of school IT systems, networks, devices and accounts
- Personal devices used on the school network (BYOD)
- Remote learning and home access platforms
- AI tools accessed in school or for school related activity

Definitions

Online Safety: The practice of protecting users from online risks including harmful content, contact, conduct and commerce.

Artificial Intelligence (AI): Computer systems that perform tasks requiring human intelligence, including generative AI tools that create text, images, audio, video or code (e.g. ChatGPT, Microsoft Copilot, Google Gemini).

Generative AI: AI systems trained on large datasets to generate new content and responses.

Safeguarding children is defined in [Working together to safeguard children](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2) <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) <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 accidentally 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) Statutory and Regulatory Framework

3.1 This policy is informed by and operates in conjunction with:

- Keeping Children Safe in Education (2025)
- Online Safety Act
- DfE: Generative Artificial Intelligence in Education
- UK GDPR and Data Protection Act 2018
- Education for a Connected World Framework
- Prevent Duty
- Behaviour Policy, Safeguarding Policy, Acceptable Use Policies

(4) Roles and Responsibilities

4.1 Governing Body

- Ensures statutory compliance with online safety and AI safeguarding
- Receives regular updates on online safety risks and incidents
- Approves this policy and reviews its effectiveness annually

4.2 Headteacher and Senior Leadership Team

- Ensure a whole-school approach to online safety
- Approve all pupil-facing AI tools before use
- Ensure staff training includes AI-related safeguarding risks

4.3 Designated Safeguarding Lead (DSL)

- Leads on online safety and AI-related safeguarding
- Responds to incidents involving:
 - Harmful or inappropriate content
 - AI-generated abuse, harassment or deepfakes
 - Misinformation, disinformation and conspiracy content
- Works with IT providers to ensure filtering and monitoring include AI platforms
- Ensures concerns are logged, escalated and referred where necessary

4.4 Staff

- Model safe and responsible online behaviour
- Do not enter personal or sensitive data into AI tools
- Supervise student use of technology and AI
- Report online safety concerns immediately to the DSL

4.5 Students

- Use technology and AI safely, respectfully and for educational purposes only
- Do not attempt to bypass filters or monitoring
- Report concerning content or behaviour to a trusted adult

4.6 Parents and Carers

- Are supported through guidance and communication on online and AI safety
- Are encouraged to reinforce safe online behaviour at home

(5) Artificial Intelligence (AI) – Safe and Responsible Use

5.1 AI offers educational benefits but introduces new safeguarding risks, including:

- Exposure to inaccurate or harmful content
- Over-reliance on AI outputs
- Data protection breaches
- Academic integrity issues
- Deepfakes and impersonation

5.2 The school ensures that:

- All AI tools used are risk-assessed and approved
- Filtering and monitoring systems apply to AI searches, prompts and outputs
- AI does not replace professional judgement in teaching or safeguarding
- Students are taught to critically evaluate AI-generated content

5.3 AI must not be used to:

- Generate harmful, abusive, sexualised or extremist content
- Create misinformation or impersonation content
- Circumvent school rules or assessments
- Upload personal or identifiable data

(6) Filtering and Monitoring

6.1 The school maintains robust filtering and monitoring systems that:

- Block access to harmful and inappropriate content
- Monitor searches, activity and AI use
- Alert designated staff to safeguarding risks
- Are reviewed regularly in line with emerging threats

6.2 Filtering and monitoring apply to:

- School devices
- Personal devices on the school network
- AI platforms accessed for school use

(7) Online Safety Education

7.1 Online safety education is embedded across:

- Computing
- PSHE and RSHE
- Assemblies and tutor time
- Sixth Form study skills and enrichment

7.2 Students are taught about:

- Safe online relationships
- Cyberbullying and harassment
- Misinformation, disinformation and conspiracy theories

- Ethical and responsible use of AI
- How to seek help and report concerns

(8) Reporting and Responding to Incidents

8.1 All online safety concerns must be reported to the DSL immediately.

8.2 The school will:

- Take swift and proportionate action
- Provide support to affected students
- Involve parents/carers where appropriate
- Refer to external agencies where required (e.g. MASH, police, CEOP)

8.3 No staff member should investigate independently.

(9) The Internet

- 9.1 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.
- 9.2 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.
- 9.3 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.

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

- 10.1 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.
- 10.2 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.
- 10.3 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.

- 10.4 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.
- 10.5 We advise that Campus email addresses should not be used for setting up personal social media accounts or to communicate through such media.
- 10.6 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.
- 10.7 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_0IPs084

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

- 10.8 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
- 10.9 See Appendix 2 'Guidelines for creating and maintaining social media accounts'

(11) Email

- 11.1 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.
- 11.2 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.
- 11.3 Users must not knowingly send or receive information that will bring the Campus into disrepute.
- 11.4 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) Mobile Phones and other devices

12.1

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.

- 12.2 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.
- 12.3 Students should report any instances of unwanted or distressing text messages to their Tutor or relevant member of staff.
- 12.4 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.
- 12.5 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.
- 12.6 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.

(13) Publish Student's Images and Work

- 13.1 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.
- 13.2 If students do not wish to have their photographs taken, they can opt out and this choice should be communicated with the students.
- 13.3 Work can only be published with the written permission of the student.

(14) Use of Photographs and Video

- 14.1 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.
- 14.2 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.
- 14.3 Staff must be fully aware of the consent form responses from Parent/Carers when considering use of images.

- 14.4 Staff should always use a Campus camera to capture images and should not use their personal devices.
- 14.5 Photographs taken by the Campus are subject to the Data Protection Act.

(15) Photographs and Videos taken by Parents/Carers

- 15.1 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.
- 15.2 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.

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

- 16.1 Landau Forte Academy Sixth Form/QEMS is committed to preventing people from being drawn into anything that may encourage or support harm.. 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.

(17) Dealing with Bullying issues

- 17.1 The Campus's Online Safety Policy and/or Anti-bullying Policy should make clear the sanctions regarding bullying using new technologies.
- 17.2 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.
- 17.3 Use of social networking sites to harass, bully or intimidate would be covered by this irrespective of when/where the post was made.

(18) Reporting

- 18.1 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.
- 18.2 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.

(19) Breaches of this Policy

- 19.1 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.

(20) Handling Online Safety Complaints

- 20.1 Complaints of Internet misuse will be dealt with by a member of Senior Leadership Team.
- 20.2 Complaints concerning safeguarding issues will be dealt with according to the Campus Safeguarding Policy.
- 20.3 Students and Parents/Carers will be informed of the complaints procedure.

(21) Relevant Legislation

- 21.1 Data Protection Act 1998
- 21.1.1 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.
- 21.1.2 Under the Act, each Campus is a separate data user and must complete a "Notification" each year.
- 21.1.3 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.
- 21.2 Computer Misuse Act 1990
- 21.2.1 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
- 21.3 Copyright, Designs and Patents Act 1988
- 21.3.1 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.
- 21.3.2 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.

- 21.3.3 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.
- 21.3.4 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.
- 21.3.5 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.
- 21.3.6 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.
- 21.3.7 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.

21.4 Freedom of Information

- 21.4.1 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.
- 21.4.2 The principle behind the Act is that all information held in any format is accessible, unless certain conditions or exemptions apply.

21.5 Human Rights

- 21.5.1 The Campus must act in a way that is compatible with and promotes individuals' rights in accordance with the Human Rights Act 1998.
- 21.5.2 Definitions of Personal Information and Sensitive Personal Information for this purpose are:
 - 21.5.2.1 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
 - 21.5.2.2 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
 - 21.5.2.3 Other data - that should be protected includes: national insurance number, bank account details, credit card

(21) Handling Online Safety Complaints

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

(22) 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
- Trust Policy T035 Staff Acceptable Use Policy

(23) Policy Review

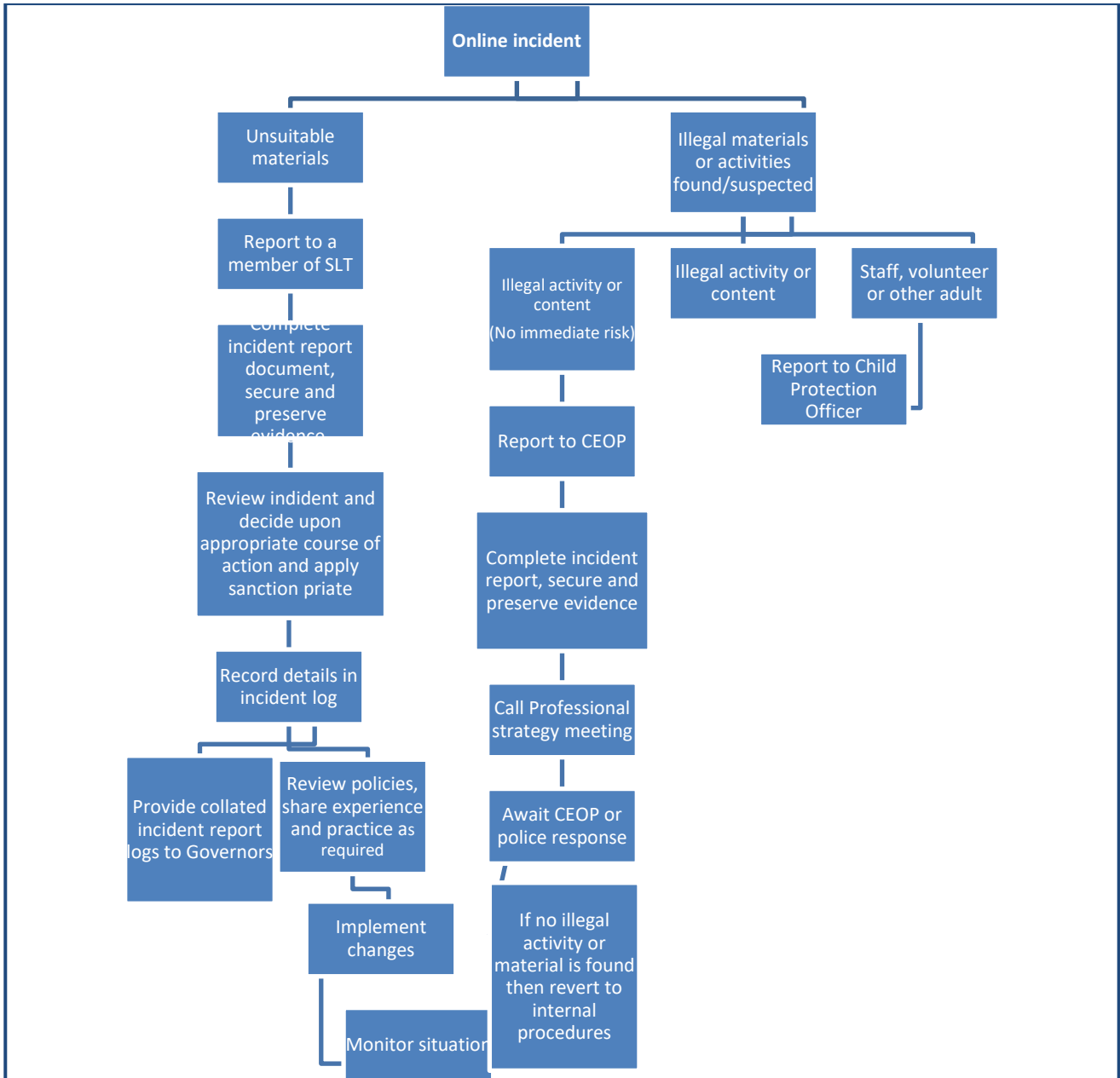
23.1 This policy will be reviewed:

- Annually
- Following serious incidents
- In response to national guidance updates relating to online safety or AI

Appendix I Responsibilities for Online Safety

Role	Name	Job Title
Member of Senior Leadership Team responsible for Online Safety	Mrs K Adams	Principal
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



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.



LANDAU
FORTE
CHARITABLE
TRUST

Date	September 2025
Change Made	Various
Made By	Miss C Wright