LEITHS EDUCATION

Online Safety Policy

Author/reviewer responsible:	Louise Kissane
Date of last review:	September 2026
Next review date:	September 2027
Lead for review:	DSL
IT Consultant:	Morcan IT Solutions

Contents

Online Safety Policy 1
1. Context 3
2. Purpose and Aims 4
3. Scope 4
4. Online Safety Risks 5
5. Online Safety and Adult Safeguarding 5
6. Reporting Online Safety Concerns 6
7. Low-Level Online Safety Concerns 7
8. Online Allegations Against Staff or Other Adults 7
9. Student-to-Student Online Behaviour 8
10. Sexual Harassment and Sexual Abuse Online 9
11. Sharing Intimate Images and Sexual Content 9
12. Online Bullying and Harassment 10
13. Social Media 10
14. Professional Boundaries Online 11
15. Digital Images and Video 11
16. Data Protection and Information Security 12
17. Cloud Platforms and Online Systems 13
18. Filtering and Monitoring 13
19. Device Usage 13
20. Network and Internet Access 14
21. Cybersecurity 14
23. Online Radicalisation and Prevent 15
24. Online Safety and Recruitment 15
25. Responding to an Online Safeguarding Disclosure 15
26. Recording Online Safety Concerns 16
27. Confidentiality and Information Sharing 16
28. Children Occasionally Present at Leiths 17
29. Roles and Responsibilities 17
30. Review and Monitoring 20
31. Related Policies and Documents 20

1. Context

Leiths Education recognises that online safety is an integral part of safeguarding and applies to the whole Leiths community. Online activity can create risks of abuse, exploitation, harassment, bullying, discrimination, financial harm, fraud, radicalisation, coercion, inappropriate relationships, breaches of privacy and other forms of harm.

Leiths primarily provides education to students aged 18 and above. Accordingly, this Online Safety Policy is primarily aligned with the **Adult Safeguarding Policy**, the principles of the **Care Act 2014**, the Mental Capacity Act 2005 where applicable, and Leiths' wider safeguarding arrangements.

The fact that Leiths students are adults does not remove the school's responsibility to take appropriate action where an adult student may be experiencing or be at risk of abuse, neglect or exploitation, particularly where they have care and support needs and may be unable to protect themselves from that risk.

The Adult Safeguarding Policy establishes the principles of empowerment, prevention, proportionality, protection, partnership and accountability. These principles apply equally to online safeguarding.

Leiths also recognises that children may occasionally be present on site or participate in Leiths-related activities. Where an online safety concern relates to a child, the appropriate child safeguarding procedures will apply alongside this policy.

This policy should therefore be read alongside the:

- Adult Safeguarding Policy
- Safeguarding and Child Protection arrangements applicable to children who may occasionally be present
- Low-Level Concerns Policy
- Staff Code of Conduct
- Student Handbook
- Anti-Bullying Policy & Procedure
- Complaints Policy
- Misconduct & Disciplinary Procedure
- Whistleblowing Policy
- Safer Recruitment Policy

2. Purpose and Aims

The purpose of this policy is to ensure that Leiths provides a safe, respectful and appropriately managed digital environment for students, staff, directors, contractors, volunteers and visitors.

The policy aims to:

- promote safe, responsible and respectful use of digital technology;
- establish clear expectations for online behaviour;
- recognise online abuse and other digital risks as safeguarding matters;
- ensure that concerns are identified, reported, recorded and acted upon appropriately;
- protect adult students from online abuse, neglect, exploitation and other harm;
- support students to exercise autonomy and make informed decisions about their online activity;
- protect staff and other members of the Leiths community from inappropriate online behaviour;
- ensure professional boundaries are maintained online as well as offline;
- provide clear arrangements for responding to online safeguarding concerns involving staff or other adults;
- support effective data protection and information security;
- ensure that filtering and monitoring arrangements are proportionate and appropriate;
- support the Prevent duty and awareness of online radicalisation and extremism;
- provide appropriate arrangements where a child is occasionally present; and
- protect the reputation, integrity and professional standards of Leiths.

Online behaviour is subject to the same standards of professionalism, respect and safeguarding as behaviour taking place face-to-face. These expectations apply whether activity takes place on Leiths premises, remotely, during or outside normal working hours, and whether a Leiths-owned or personal device is being used.

3. Scope

This policy applies to all members of the Leiths community, including:

- students, staff, support, directors, volunteers, contractors, consultants, external service providers and visitors using Leiths technology or systems.

It applies to:

- Leiths-owned devices;
- personal devices when used for Leiths-related activity;

- Leiths email and Microsoft 365 systems;
- Teams and other approved communication platforms;
- social media;
- cloud-based systems;
- online learning resources;
- messaging applications;
- websites and online services; and
- digital activity undertaken away from the Leiths premises where it has a connection to the Leiths community or affects the safety or wellbeing of a member of that community.

4. Online Safety Risks

Online risks can be considered under four broad areas:

Content - Exposure to harmful, illegal, discriminatory, violent, sexually explicit or otherwise inappropriate material.

Contact - Unwanted or inappropriate contact, grooming, coercion, harassment, exploitation, manipulation, scams or inappropriate relationships.

Conduct - Bullying, harassment, abuse, discriminatory behaviour, harmful sexual behaviour, intimidation, impersonation, inappropriate communications, misuse of social media or breaches of professional boundaries.

Commerce - Fraud, financial exploitation, scams, identity theft, coercive financial activity and other forms of online financial harm.

These categories may overlap. A single incident may involve several forms of risk and may also constitute an adult safeguarding concern, a disciplinary matter, a criminal matter or a data protection incident.

Staff should not attempt to determine the final classification of a concern themselves. Where there is uncertainty, the concern should be reported to the DSL or DDSL.

5. Online Safety and Adult Safeguarding

Online safety concerns involving an adult student must be considered within the framework of the Adult Safeguarding Policy.

A concern should be considered as a potential adult safeguarding matter where there is information suggesting that an adult:

- has needs for care and support;
- is experiencing, or is at risk of, abuse or neglect; and

- because of those needs is unable to protect themselves against the abuse, neglect or risk of it.

Not every online safety incident will meet this threshold. Many matters may appropriately be dealt with through pastoral support, the Student Handbook, complaints procedures, disciplinary procedures or other internal processes.

However, an online incident must not be dismissed simply because it occurs away from Leiths or through a personal device.

Where there is any indication that an adult student may be experiencing abuse, neglect, exploitation or serious harm, the matter must be reported to the DSL or DDSL without delay.

The DSL will consider:

- the student's wishes and desired outcomes;
- whether the student has capacity to make relevant decisions;
- whether consent should be sought;
- whether immediate protective action is required;
- whether the circumstances meet or may meet the Care Act safeguarding criteria;
- whether advice or referral to Adult Social Care is appropriate;
- whether another agency needs to be involved; and
- whether other Leiths policies or procedures should also be initiated.

The principles of **Making Safeguarding Personal** apply. Adult students should, wherever possible, be involved in decisions about what happens next and their wishes, feelings and outcomes should be central to the response.

6. Reporting Online Safety Concerns

All members of the Leiths community are expected to report online safety concerns promptly.

A concern should be reported to:

Designated Safeguarding Lead:
Louise Kissane

Deputy Designated Safeguarding Leads:
Matt Beavis / Sophie Kidd

Where the concern relates to a member of staff, the reporting arrangements in the Adult Safeguarding Policy and Low-Level Concerns Policy must be followed.

Where the concern relates to the DSL or a member of the safeguarding team, it must be escalated in accordance with the Adult Safeguarding Policy.

Where the concern relates to the Culinary School Director or CEO, it should be reported to the Board member with responsibility for safeguarding, in accordance with the relevant safeguarding and whistleblowing procedures.

Staff should **always report a concern where they are unsure whether it constitutes a safeguarding matter**. It is the responsibility of the DSL/DDSL to assess the information and determine the appropriate response.

7. Low-Level Online Safety Concerns

Online behaviour may constitute a low-level concern where it causes a sense of unease or a "nagging doubt" about whether an adult working in or on behalf of Leiths has acted consistently with the Staff Code of Conduct, professional expectations or appropriate safeguarding practice.

Examples may include:

- inappropriate online communication with a student;
- communicating with students through personal accounts where this is not appropriate;
- unnecessary or inappropriate direct messaging;
- inappropriate social media interactions;
- excessive familiarity or blurred professional boundaries;
- sharing inappropriate content;
- inappropriate comments, jokes or language;
- conduct that is unprofessional but does not meet the threshold for a safeguarding allegation; or
- behaviour which, when considered alongside other information, may indicate a developing pattern.

All such concerns must be reported in accordance with the **Low-Level Concerns Policy**.

A low-level concern must **not** be used where the circumstances indicate abuse, exploitation, neglect, serious misconduct or another safeguarding concern. In those circumstances, the matter must be escalated under the Adult Safeguarding Policy and/or allegations procedures.

Patterns of apparently low-level online behaviour may become significant when considered collectively. The DSL/DDSL will therefore ensure that relevant concerns are recorded and reviewed for patterns or escalation.

8. Online Allegations Against Staff or Other Adults

Where an online incident involves an allegation that a member of staff, volunteer, contractor or other adult working on behalf of Leiths:

- has harmed or may have harmed an adult student;
- has committed a criminal offence;

- has behaved in a way which may indicate that they are unsuitable to work with students; or
- may have placed an adult student at risk of abuse, neglect or exploitation,

the matter must be reported immediately to the DSL or appropriate senior person in accordance with the **Allegations Management** section of the Adult Safeguarding Policy.

The DSL will determine, with appropriate advice where necessary, whether the matter requires:

- adult safeguarding action;
- referral to Adult Social Care;
- police involvement;
- disciplinary investigation;
- complaints procedures;
- management action;
- a low-level concern response; or
- another appropriate course of action.

Any investigation must be proportionate and must not compromise safeguarding or any potential criminal investigation.

9. Student-to-Student Online Behaviour

Leiths recognises that online interactions between students can result in:

- bullying;
- harassment;
- sexual harassment;
- unwanted sexual communications;
- threats or intimidation;
- discriminatory abuse;
- sharing of private information or images;
- impersonation;
- coercive or controlling behaviour;
- financial exploitation;
- exclusion or social isolation; and
- other forms of harmful conduct.

Because Leiths students are adults, such incidents should be considered within the context of adult safeguarding, the Student Handbook, complaints procedures and other relevant Leiths processes.

Where a student may be experiencing abuse, exploitation or serious harm, the DSL must be informed.

Where the incident does not constitute safeguarding, it should nevertheless be addressed appropriately and promptly under the relevant Leiths procedures.

Leiths will not dismiss harmful behaviour as "banter" where it causes or may cause harm.

10. Sexual Harassment and Sexual Abuse Online

Online sexual harassment or abuse may include:

- unwanted sexual messages;
- sexualised comments;
- sending unwanted sexual images;
- requests for sexual images;
- coercion to share images;
- threats to share intimate images;
- non-consensual sharing of intimate images;
- online grooming or manipulation;
- sexualised bullying; or
- sexual harassment through social media or messaging groups.

Any such concern should be reported to the DSL/DDSL.

Where the person affected is an adult student, the response will be guided by the Adult Safeguarding Policy, including consideration of consent, capacity, wishes and desired outcomes.

Where a child is involved, the relevant child safeguarding procedures must be followed.

11. Sharing Intimate Images and Sexual Content

Students should be encouraged to seek help if they have been pressured, coerced or manipulated into creating, receiving or sharing intimate images.

Staff must not:

- forward an intimate image;
- copy or download an image unnecessarily;
- share an image with colleagues who do not need to see it;
- ask a student to forward an image to them; or
- investigate beyond what is necessary to establish immediate safeguarding information.

The concern should be reported to the DSL/DDSL, who will determine appropriate action.

Where an adult student has capacity to make relevant decisions, their wishes and consent should normally be central to the response. However, information may be shared without consent where this is lawful and necessary, including where there is serious or imminent risk of harm, a risk to another person, serious crime, lack of relevant capacity, a legal obligation or another lawful basis.

All decisions regarding consent and information sharing must be appropriately recorded.

Where the incident involves a child, the child safeguarding procedure must be followed.

12. Online Bullying and Harassment

Online bullying and harassment can take place through:

- social media;
- messaging applications;
- email;
- group chats;
- online forums;
- gaming platforms;
- learning platforms; and
- other digital communications.

Online bullying may occur outside Leiths and outside normal school hours but may nevertheless affect a student's safety, wellbeing or ability to participate in education.

Concerns should be reported to an appropriate member of staff and, where there is a safeguarding element, to the DSL/DDSL.

The Anti-Bullying Policy, Student Handbook and Adult Safeguarding Policy should be considered as appropriate.

13. Social Media

Leiths recognises that social media is an established part of modern life. All members of the Leiths community are expected to behave respectfully and professionally online. The same standards of conduct apply online as apply in person.

Members of the Leiths community must not use social media to:

- bully, harass or intimidate another person;
- discriminate against another person;
- share confidential or personal information without lawful authority;
- publish abusive or threatening material;
- share inappropriate images of students or colleagues;

- undermine professional boundaries;
- impersonate another person;
- disclose safeguarding information;
- bring Leiths or members of its community into serious disrepute; or
- engage in conduct that may place another person at risk.

Students are encouraged to use appropriate Leiths channels when communicating about their course.

Any social media activity that may constitute a safeguarding concern should be reported to the DSL/DDSL. Where the concern relates to a member of staff, the Staff Code of Conduct, Low-Level Concerns Policy and Adult Safeguarding Policy should also be considered.

14. Professional Boundaries Online

Staff must maintain clear and appropriate professional boundaries when communicating with students.

Staff should:

- use professional Leiths accounts rather than personal accounts
- avoid private communications
- maintain appropriate records of significant communications where necessary
- report accidental or inappropriate communications to the DSL/DDSL where safeguarding or professional boundaries may be relevant.

There should be no circumstances where a private email account is intentionally used by staff to communicate with a student for Leiths business.

If a private communication occurs accidentally, the circumstances should be reported promptly so that an appropriate decision can be made about whether further action is required.

15. Digital Images and Video

Images and videos of students must be handled in accordance with the Data Protection Policy and applicable consent arrangements.

Where images are captured for Leiths purposes:

- the purpose should be appropriate and legitimate
- students' privacy should be respected
- images should not be taken secretly
- images should not be used for purposes for which appropriate permission has not been obtained

- images should be stored on approved Leiths systems
- unnecessary copies should not be retained
- personal devices should not be used for long-term storage
- images should be deleted from personal devices and associated cloud backups once securely transferred to approved storage.

Staff may occasionally use personal phones to capture photographs or videos for legitimate Leiths activities, but this should be open, appropriate and connected to the activity taking place. Images should be transferred to approved Leiths storage as soon as reasonably possible and deleted from the personal device and associated cloud storage.

The Staff Code of Conduct applies to all staff use of personal devices.

Students should not photograph or record staff or other students in circumstances where this would be intrusive, inappropriate or contrary to Leiths rules.

16. Data Protection and Information Security

Online safeguarding and data protection are closely connected.

Safeguarding information is highly sensitive and must be:

- accessed only by those with an appropriate need to know
- stored securely
- shared only through approved systems
- handled in accordance with the Data Protection Policy
- retained in accordance with the applicable retention schedule
- shared externally only where there is an appropriate lawful basis.

Data protection legislation should not be used as a reason to prevent necessary safeguarding information sharing.

For adult safeguarding matters, the principles and information-sharing provisions contained within the Adult Safeguarding Policy apply.

Where information is shared without the student's consent, the DSL should record:

- what information was shared
- with whom
- why it was shared
- the lawful basis or safeguarding justification
- why consent was not sought, where applicable.

17. Cloud Platforms and Online Systems

Only approved systems should be used to store or process Leiths information.

The Data Protection Officer is responsible for ensuring that appropriate data protection considerations are applied to new systems.

Staff and students should understand:

- what information may be stored
- who can access information
- how information can be shared
- the difference between personal and organisational accounts
- the risks of inappropriate sharing
- the importance of secure passwords and authentication.

Open or widely accessible folders must not be used to store confidential or sensitive safeguarding information.

18. Filtering and Monitoring

Leiths will maintain appropriate filtering and monitoring arrangements to reduce exposure to harmful or inappropriate online content.

The DSL will work with the IT provider and DPO to:

- understand the filtering and monitoring arrangements
- review their effectiveness
- ensure safeguarding risks identified through monitoring are appropriately escalated
- report relevant information to the Board.

Filtering and monitoring arrangements must be proportionate to Leiths' adult educational environment and must take account of students' autonomy and legitimate educational access.

Monitoring must not be regarded as a substitute for staff vigilance, professional judgement or the reporting of safeguarding concerns.

19. Device Usage

Students

Students may bring mobile phones and other personal devices to Leiths. During demonstrations and formal teaching sessions, phones should remain on silent unless the teacher has given permission for their use. In kitchens, phones should only be used where permitted for legitimate purposes such as photographing students' own food.

Students must not use devices to:

- record others without appropriate permission
- access inappropriate or illegal material
- bully or harass others
- share confidential information
- breach copyright or data protection requirements
- otherwise breach the Student Handbook.

Staff

Staff working directly with students should keep personal phones on silent and use them in private staff areas during school hours unless there is a legitimate reason for use.

Student or confidential staff information must not be downloaded onto personal devices unless specifically authorised and appropriately protected.

Contractors, Volunteers and Directors

Personal devices should not be used inappropriately in the presence of students.

Photography or recording for legitimate operational purposes should be authorised where appropriate and should comply with data protection and safeguarding requirements.

20. Network and Internet Access

Students may access the Leiths wireless network for educational purposes and limited personal use within the Student Handbook. Staff, contractors and visitors must use network access in accordance with their authorised permissions.

All users are expected to:

- use appropriate security measures
- avoid accessing illegal or inappropriate material
- comply with copyright requirements
- avoid downloading malicious software
- report suspected phishing or security incidents
- comply with Leiths' Acceptable Use requirements.

Use of Leiths IT systems may be monitored in accordance with applicable policies and law.

21. Cybersecurity

Cybersecurity is an important component of online safeguarding.

Staff and students should be alert to:

- phishing, malicious links, malware, fraudulent requests, identity theft

Suspected cybersecurity incidents should be reported promptly to the appropriate IT contact and, where personal safety, safeguarding or sensitive information may be involved, to the DSL/DPO as appropriate.

23. Online Radicalisation and Prevent

Leiths recognises that the internet can be used to expose individuals to extremist material, radicalising narratives and harmful ideologies. Online activity that raises concerns about radicalisation or terrorism should be reported to the DSL.

The DSL will consider the matter in accordance with Leiths' Prevent arrangements and relevant safeguarding procedures. Staff should not attempt to investigate suspected radicalisation themselves.

24. Online Safety and Recruitment

Online information may form part of appropriate recruitment due diligence where this is identified within Leiths' Safer Recruitment Policy.

Any online search undertaken as part of recruitment must be:

- proportionate, consistent, relevant to the recruitment process, appropriately recorded and handled in accordance with data protection requirements.

The existence of online information should not automatically be interpreted as evidence of unsuitability. Decisions must be based on relevant and appropriately assessed information.

25. Responding to an Online Safeguarding Disclosure

If a student or other person reports an online safeguarding concern, staff should:

1. listen calmly
2. take the concern seriously
3. allow the person to explain what has happened
4. avoid judgement or victim-blaming
5. avoid promising confidentiality
6. establish only the information necessary to respond safely
7. avoid viewing, forwarding or copying harmful material unnecessarily
8. report the concern to the DSL/DDSL without delay
9. make a factual record of the concern
10. follow any further instructions from the DSL.

Staff should not conduct their own investigation.

Where an adult student makes a disclosure, the student's wishes and desired outcomes should be considered in accordance with the Adult Safeguarding Policy.

---

26. Recording Online Safety Concerns

Online safety concerns that have a safeguarding element must be recorded in accordance with the safeguarding recording arrangements.

Records should be:

- contemporaneous where possible
- factual and objective
- dated and timed
- clear about who provided the information
- clear about whether information is first-hand or second-hand
- clear about actions taken
- clear about decisions regarding consent and information sharing
- stored securely

The DSL will consider whether information should also be recorded in:

- the safeguarding log
- the Low-Level Concerns log
- a student pastoral record
- an HR record
- a disciplinary record

The existence of an online incident does not automatically mean that it is a safeguarding incident. The DSL will determine the appropriate recording route.

---

27. Confidentiality and Information Sharing

Safeguarding information must be treated confidentially and shared on a need-to-know basis.

Staff must not discuss safeguarding concerns through:

- personal messaging groups
- social media
- informal staff groups

- personal email accounts

Where information needs to be shared to protect an adult or child, appropriate information may be shared lawfully and proportionately.

Staff should never allow concerns about data protection to prevent necessary safeguarding action. The Adult Safeguarding Policy sets out the circumstances in which information may be shared without consent.

---

28. Children Occasionally Present at Leiths

Leiths is an adult educational setting. However, children may occasionally be present on site or involved in Leiths-related activities.

Where an online safety concern relates to a child:

- the child safeguarding procedures must be followed
- the DSL must be informed immediately
- relevant child safeguarding legislation and guidance must be considered
- information must be shared with appropriate children's safeguarding agencies where required
- staff must follow any additional arrangements relating to children set out in Leiths' safeguarding procedures

The fact that the majority of Leiths students are adults does not remove the requirement to act appropriately where a child is present or affected.

---

29. Roles and Responsibilities

29.1 All Staff

All staff are responsible for:

- reading and following this policy
- understanding that online safety is part of safeguarding
- modelling appropriate online behaviour
- maintaining professional boundaries
- reporting online safeguarding concerns promptly
- reporting low-level concerns about adults
- protecting confidential information
- following acceptable-use requirements

- using approved systems
- maintaining appropriate cybersecurity
- attending safeguarding and online safety training
- raising concerns where online safety arrangements are not working effectively

Staff should also report patterns, trends or emerging risks to the DSL rather than assuming that someone else will do so.

29.2 Designated Safeguarding Lead

The DSL has lead responsibility for safeguarding and will:

- provide advice and support to staff
- assess online safeguarding concerns
- determine whether the Adult Safeguarding Policy applies
- consider referrals to Adult Social Care or other agencies
- consider capacity and consent
- ensure appropriate safeguarding records are maintained
- monitor low-level concerns and safeguarding trends
- liaise with the DPO and IT provider
- oversee filtering and monitoring
- ensure online safety training is provided
- maintain awareness of emerging online risks
- ensure Prevent-related online risks are considered
- review this policy annually
- provide appropriate anonymised reporting and assurance to the Board

The DSL may delegate specific operational tasks but retains overall safeguarding responsibility. DDSL's will support the DSL in all aspects of online safeguarding.

29.3 Board Member with Responsibility for Safeguarding

The Board safeguarding representative will:

- provide strategic oversight
- approve and review this policy
- provide challenge regarding online safeguarding arrangements

---

- review anonymised safeguarding and online safety information
- ensure concerns about senior leaders are appropriately escalated

---

29.4 Data Protection Officer

The DPO will:

- advise on the lawful processing and storage of personal data
- support appropriate information-sharing arrangements
- oversee data protection considerations relating to online systems
- advise on data breaches
- support the secure handling of safeguarding information
- work with the DSL and IT provider to ensure safeguarding and data protection requirements are appropriately balanced.

29.7 IT Provider

The IT provider will support Leiths by:

- maintaining appropriate technical security
- monitoring and maintaining filtering arrangements
- supporting cybersecurity
- identifying technical risks
- advising on emerging online threats
- supporting incident response
- working with the DSL and DPO as appropriate.

29.8 Students

Students are expected to:

- read and follow the Student Handbook and relevant acceptable-use requirements
- behave respectfully online
- maintain appropriate boundaries with staff and other students
- protect their own and others' privacy
- report abuse, harassment, exploitation or other harmful behaviour
- report concerns about staff or other members of the Leiths community

---

- use approved Leiths systems appropriately
- protect passwords and personal information
- avoid sharing images or information about others without appropriate permission
- seek support where they feel unsafe, pressured, exploited or harmed online

---

30. Review and Monitoring

This policy will be reviewed annually and sooner where:

- legislation or guidance changes
- significant online safety incidents occur
- new technology or systems are introduced
- safeguarding risks change
- monitoring identifies emerging trends

The DSL will review relevant incident records, low-level concerns, safeguarding information and filtering/monitoring information to identify patterns and emerging risks.

The Board will receive appropriate anonymised information to provide strategic oversight and challenge.

---

31. Related Policies and Documents

This policy should be read alongside:

1. Adult Safeguarding Policy 2026/27
2. Low-Level Concerns Policy
3. Staff Code of Conduct
4. Student Handbook
5. Data Protection Policy
6. Anti-Bullying Policy
7. Complaints Procedure
8. Disciplinary Procedure
9. Whistleblowing Policy
10. Safer Recruitment Policy
11. Safeguarding Concern Log
