LEITHS

SCHOOL OF FOOD AND WINE

Online Safety Policy

Written	April 2023
Reviewed	January 2024
Next Review Date	January 2025
Lead for Review	DSL
IT Consultant	ian.price@fallstreak.co.uk

Contents

Context

Whilst the curriculum at Leiths School of Food and Wine (Leiths) does not encompass RSHE, we acknowledge our duty to keep children safe and we therefore reflect updates in Keeping Children Safe in Education (September 2023) calling for greater collaboration and dialogue between safeguarding, leadership and technical teams. These include highlighting strategic responsibilities around filtering and monitoring, providing safeguarding training for all directors and reminders on the use of appropriate language. We also include mentions of carrying out an online safety audit and online searches as part of the recruitment process, as reflected in our Safer Recruitment Policy.

Leiths requires all staff and students to adhere to our guidelines on acceptable use as outlined in the Student Handbook and Staff Code of Conduct. This is reviewed at least annually so as to enforce correct safeguarding.

Online safety is an integral part of safeguarding and accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE) and sits alongside our Safeguarding Policy. Any issues and concerns with online safety must always follow Leiths' Safeguarding and Child Protection procedures.

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area and reflects teachers' day-to-day experiences pertinent to online safety.

What are the current main online safety risks

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 136 of KCSIE 2023). These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all three. This is evident in Ofcom's Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other aps and sites.
KCSIE 2023 highlights additional risks e.g., extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families, including sexual and criminal exploitation, serious youth violence, upskirting and "sticky design" where games and social media companies persuade users to stay online.

We monitor sites such as Everyone's Invited where Leiths is not listed, and we discourage students from participating in such sites.

Following the Ofsted review into **peer-on-peer sexual abuse**, Leiths follow the updated advice on sexual violence and harassment guidance, incorporated in Part 5 of KCSIE where the term 'peer-on-peer' has been replaced with 'child-on-child' which has many online implications. We ensure student have the opportunity to report sexual harassment and abuse concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately and ensure students are aware of the NSPCC helpline and our internal reporting channels.

Overview

Aims

This policy aims to promote a "whole school approach" to online safety by:

- Setting out expectations for all Leiths community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of our physical site and our working day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching and learning, increase attainment and prepare students for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with students, especially any aged under 18, to understand their roles and responsibilities to work safely and responsibly with technology and the online world: ○ for the protection and benefit of the students in their care, and ○ for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice. ○ for the benefit of the school, supporting our Leiths ethos, aims and objectives, and protecting the reputation of the school.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to the Student Handbook)

Further Help and Support

Leiths' Safeguarding Policy details how any reports or referrals should be made i.e., through the DSL, Principal or Board Member with responsibility for Safeguarding as appropriate to who is being referred.

Beyond this, the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud offer advice and details are readily available online.

Scope

This policy applies to all members of the Leiths community (including teaching and support staff, directors, volunteers, contractors, students, and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their role at Leiths.

Roles and responsibilities

Leiths is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning, and to report immediately any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. At Leiths we promote an ambiance where we learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the Leiths community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) either on Leiths' premises or from home, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites. We regularly review the appropriateness of filtering and monitoring software implemented by Morcan, our IT Provider.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and that although it is not taught explicitly as part of the curriculum at Leiths, we have due regard for online safety.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the onlinesafety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

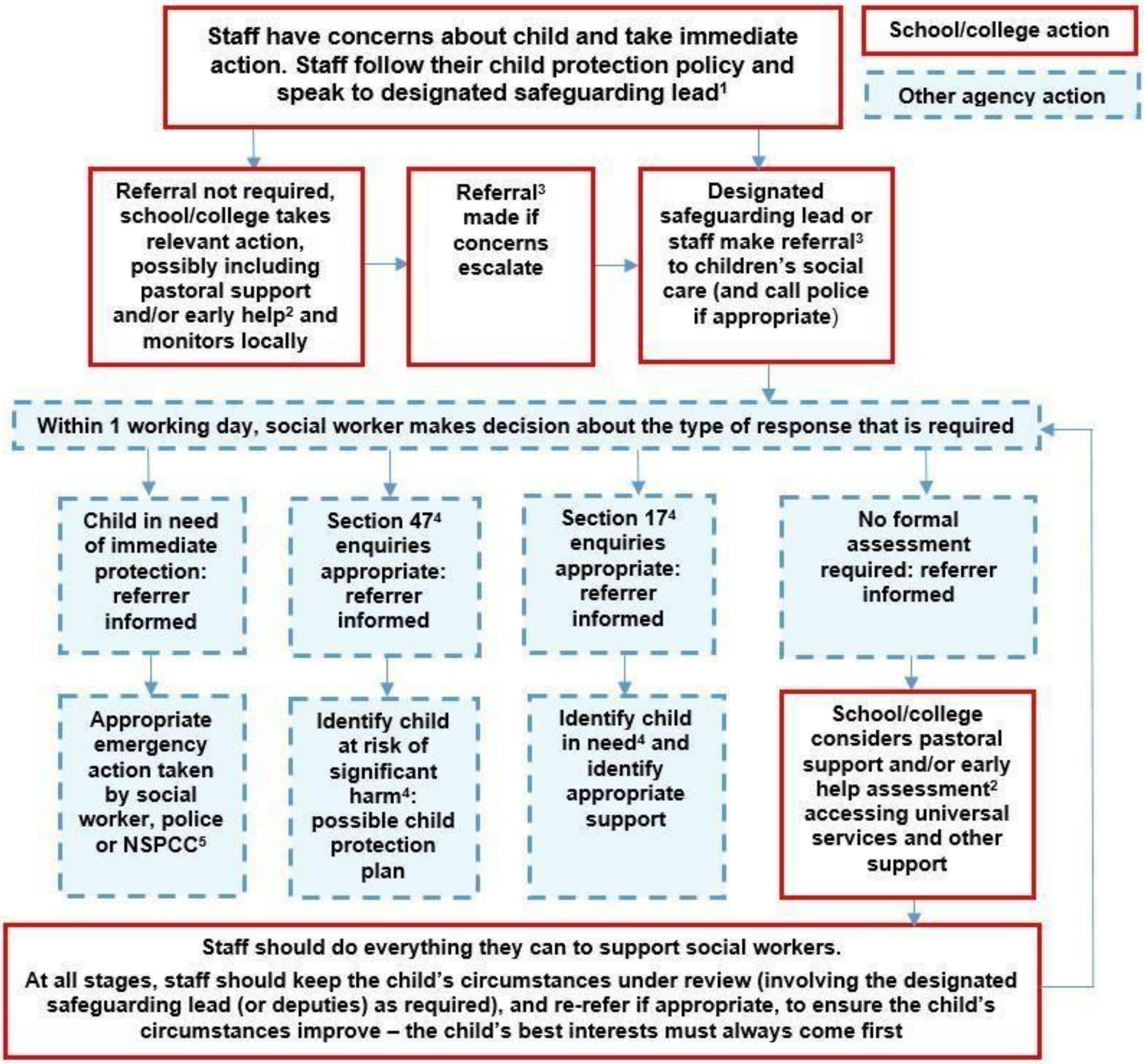
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Student Handbook
- Staff Code of Conduct
- Data Protection Policy

Leiths commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL on the same day. Any concern/allegation about staff misuse is always referred directly to the Principal, unless the concern is about the Principal in which case the complaint is referred to the Board Member who represents the Board in matters pertaining to Safeguarding, and to the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline as detailed in the Whistleblowing Policy.

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2023 as the key education safeguarding document. As outlined previously, online safety concerns are no different from any other safeguarding concern.



School/college action

Other agency action

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]

Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally

Referral[3] made if concerns escalate

Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47[4] enquiries appropriate: referrer informed

Section 17[4] enquiries appropriate: referrer informed

No formal assessment required: referrer informed

Appropriate emergency action taken by social worker, police or NSPCC[5]

Identify child at risk of significant harm[4]: possible child protection plan

Identify child in need[4] and identify appropriate support

School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support

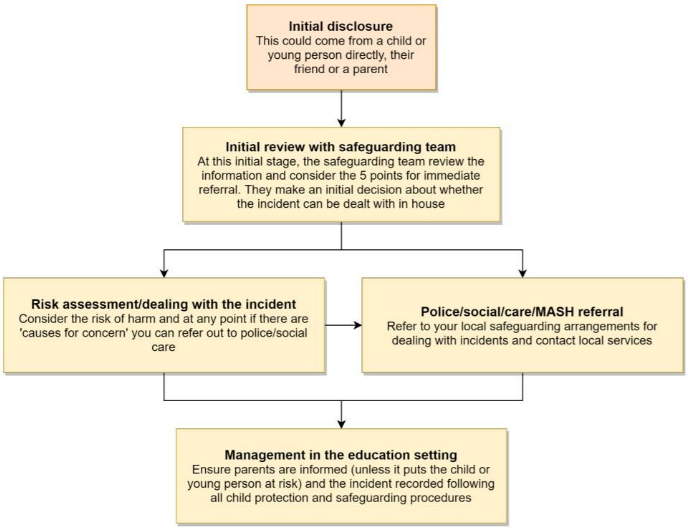
Staff should do everything they can to support social workers.

At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Sharing nudes and semi-nudes (previously known as "sexting")

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but **child sexual abuse**.

There is a one-page overview called Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) for all staff to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. The DSL will in turn use the full guidance document, Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) to decide next steps and whether other agencies need to be involved, bearing in mind that this advice pertains to children and schools rather than Further Education and over 18s.


Initial disclosure
This could come from a child or young person directly, their friend or a parent
Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house
Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care
Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services
Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst the sharing of nudes and semi-nudes may be illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area. Staff will bear in mind the 5 points above when making a decision as to whether a referral is necessary and will seek input from the DSL if in any doubt.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying. For further clarification, see the Anti-Bullying Policy and Procedure.

Sexual violence and harassment

DfE guidance on sexual violence and harassment has been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff at Leiths should work to foster a zero-tolerance culture and maintain an attitude of ***'it could happen here'***. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. It is important for staff at Leiths to communicate incidents to the DSL or a DDSL so that the log of low-level concerns about students can be updated and any patterns in behaviour or escalations followed up.

The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk . The helpline provides expert advice and support for school and college staff with regard to online safety issues.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in our Student Handbook and Staff Code of Conduct.

Where students contravene these rules, the guidance in the Student Handbook will be applied; where staff contravene these rules, action will be taken as outlined in the Staff Code of Conduct.

Further to these steps, Leiths reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour at Leiths.

Breaches will be dealt with in line with the procedures in the Student Handbook or Staff Code of Conduct as appropriate.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Leiths will request that the post be deleted and will expect this to be actioned promptly, i.e., on the same day that the request is made.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4). When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**."

All pupils, staff, directors, volunteers, and contractors at Leiths are bound by our data protection policy.

Rigorous controls on the Leiths network, firewalls and filtering all support data protection. The principal, data protection officer and directors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information. Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At Leiths, we acknowledge that "All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction." KCSIE 2023, paragraph 14.

The Board at Leiths ensures the school has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness through the Board Member with specific responsibility for Safeguarding. This Board Member liaises at least once a term with the DSL who has specific responsibility for Filtering and Monitoring and who in turn liaises directly with Morcan to be assured of the effectiveness of our systems. The Board ensures that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. The Board has appropriate awareness of the Department for Education filtering and monitoring standards: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges updated in March 2023.

At Leiths, we have a dedicated and secure internet connection that is protected with firewalls and multiple layers of security, including a web filtering system which is updated automatically by our provider, Morcan.

The DSL and IT Consultant (Ian Price) liaise regularly to review filtering and monitoring, noting any trends and assuring responses to any perceived threats to student and staff safety. The Board Member with responsibility for Safeguarding receives an overview of these meetings when she meets each term with the DSL.

The appropriateness of Leiths' filtering and monitoring systems are informed in part, by the risk assessment required by the Prevent Duty and completed by the DSL.

- There should be no circumstances where a private email is used by staff at Leiths when communicating with a student; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
    - Internally, staff should use the Leiths network, including when working from home. Office 365 and Teams are used for all communications at Leiths and there are secure private channels for confidential matters and necessary storage of personal data.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring Leiths into disrepute or compromise the professionalism of staff.
- Students and staff should be aware that all use of the Leiths IT systems can be monitored, their emails may be read, and the rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or with links to adult sites may be blocked and not arrive at their intended destination.

Leiths' website

Leiths' website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Principal and Directors have delegated the day-to-day responsibility of updating the content of the website to Victoria Prior, Marketing and Communications Director.

The Department for Education (DfE) has determined information which must be available on a school or college website and Leiths refer to this to ensure that are requirements are met. Where other staff submit information for the website, they are asked to remember:

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must be credited, and material only used with permission.
- Where student work, images or videos are published on the website, their identities are protected, and full names are not published.

Cloud platforms

The Data Protection Officer (DPO) analyses and documents systems and procedures before they are implemented, and regularly reviews them.

The following principles apply:

- Privacy statements inform students when and what sort of data is stored in the cloud.
- The DPO approves new cloud systems, what may or may not be stored in them and by whom.
- Regular training ensures all staff understand sharing functionality to ensure that student data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Students and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- In practice, students do not use the Leiths network for data storage nor have need to do so.
- Only school-approved platforms are used by students or staff to store student work.
- All stakeholders understand the difference between consumer and education products (e.g., a private email account or private One Drive and those belonging to our managed educational domain at Leiths).

Digital images and video

When a student joins Leiths, they or their fee-payer (if different) are asked if they give consent for their image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long such data will be stored.

Whenever a photo or video is taken/made, the member of staff taking it will check with the registrar that permission has not been withdrawn for its use and storage.

Any students shown in public-facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them.

All staff are governed by their contract of employment and Leiths' Staff Code of Conduct, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. At Leiths members of staff may occasionally use personal phones to capture photos or videos of students, but these will be appropriate, linked to Leiths activities, taken without secrecy and not in a one-to-one situation, and always moved to storage on the Leiths system as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos and staff are aware to delete such back-ups).

Photos are stored on the school network in line with the retention schedule of our Data Protection Policy.

Staff and students are reminded annually about the importance of not sharing without permission, due to reasons of child protection and safeguarding, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage students to think about their online reputation and digital footprint, not least for their future career or placement prospects.

Social media

Leiths' SM presence

Leiths works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about Leiths online). Few prospective students will apply for a course without first 'googling' to assess what is being said online. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about us and to respond to criticism and praise in a fair, responsible manner.

Staff, and pupils' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many students and staff will use it. However, as stated in the Student Handbook and Staff Code of Conduct we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face-to-face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or staff into disrepute. This applies both to public pages and to private posts, e.g., chats, pages or groups.

If anyone has a concern about Leiths or any member of our community, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, our complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter but can cause upset to staff and students and risk undermining staff morale our reputation which is important for the students we serve.

Students are strongly discouraged from befriending staff, Board members, volunteers and contractors or otherwise communicating with them on non-Leiths' channels via social media. In the case of a student aged under 18, then this is forbidden. Given the nature of the school, its curriculum and Further Education environment, social interactions and sharing of recipes, restaurant recommendations, links to YouTube tutorials and similar are encouraged. However, the use of Leiths' WhatsApp group for such communications is strongly encouraged and etiquette in how to use this and how to report misuse is integral to the ethos of Leiths' community and communicated to students.

Any attempt to use social media in a manner that could be a safeguarding concern or disciplinary matter should be notified to the DSL or to the Principal (if by a staff member).

Device usage

Personal devices including wearable technology and bring your own device (BYOD)

- **Students** may bring mobile phones into the school for emergency use but during demonstrations and formal teaching sessions phones must remain turned off at all times, unless the teacher has given express permission otherwise as part of the lesson. Important messages for students will be passed on by the school office. In the kitchen, phones are not allowed other than for students to take photographs of their food which is likely to form part of their assessed portfolio.
- **All staff who work directly with students** should leave their mobile phones on silent and only use them in private staff areas during school hours. Student or staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, Board Members** should leave their phones in their pockets and turned off when on the premises. Under no circumstances should they be used in the presence of students or to take photographs or videos. If this is required (e.g., for contractors to take photos of equipment or buildings), permission from the Principal should be sought (she may choose to delegate this) and this should be done in the presence of a member staff.

Network / internet access on school devices

- **Students** do not have networked file access via personal devices. However, they are allowed to access the school wireless internet for school-related internet use / limited personal use within the framework of the Student Handbook guidelines. All such use is monitored.
- **All staff who work directly with students** should leave their mobile phones on silent and only use them in private staff areas during school hours.
- **Volunteers, contractors, Board Members** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Principal and staff authorised by them have a statutory power to search students aged under 18 and their property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appendix 1

All staff

Key responsibilities:

- Read and follow this policy in conjunction with Leiths' main safeguarding policy and the relevant parts of Keeping Children Safe in Education.
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident remembering to details the reasons behind any decision.
- Know who the Designated Safeguarding Lead (DSL) and Deputies are; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon.
- Sign and follow the guidelines in the Staff Code of Conduct.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage students to follow the guidelines in the Student Handbook when at home as well as here at Leiths and when on work placements too.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as *banter* - this includes bullying, sexual violence and harassment. The DSL has disseminated relevant information from the updated section in KCSIE 2023 on this.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the corridors, on the stairs or in changing rooms and other communal areas outside the classroom, kitchen or demonstration kitchen – let the DSL know.
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues.
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Principal

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding.
- Oversee and support the activities of the Designated Safeguarding Lead team and ensure they work with technical colleagues (Morcan and IT Consultant) to ensure that checks and safeguards work appropriately.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance.
- Ensure ALL staff undergo safeguarding training (including online safety and an understanding of roles with regard to filtering & monitoring) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL Directors undergo safeguarding and child protection training and updates (including online safety and an understanding of roles with regard to filtering & monitoring) to provide strategic challenge and oversight into policy and practice and that Directors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate IT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child safety first principles (through the DSL who reports on this to the Board Member with responsibility for Safeguarding).
- Ensure the DSL liaises with technical colleagues (Morcan and IT Consultant, Ian Price) on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how. Note that KCSIE 2023 strengthens the wording for this.
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process in accordance with Leiths' Safer Recruitment Procedure.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Directors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure the Leiths website meets statutory requirements.

Designated Safeguarding Lead

Key responsibilities (the DSL may delegate certain online safety duties, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- "The Designated Safeguarding Lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated".
- Ensure ALL staff undergo safeguarding and child protection training (including online safety and an understanding of roles with regard to filtering & monitoring) at induction and that this is regularly updated.
- Liaise with the Principal and Board Member for Safeguarding to ensure that ALL Directors undergo safeguarding and child protection training (including online safety and an understanding of roles with regard to filtering & monitoring) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Work with the Principal, DPO and Board members to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Complete and update annually a Prevent Risk Assessment.
- Review and update this policy, other online safety documents (e.g., the relevant sections of the Student Handbook and Staff Code of Conduct) and the strategy on which they are based (in harmony with the Student Handbook and Staff Code of Conduct, Safeguarding, Prevent and others) and submit for review to the Board Member for Safeguarding.
- Receive regular updates in online safety issues and legislation.
- Communicate regularly (usually each term) with SLT and the designated safeguarding and online safety director (Caroline Waldegrave) to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure KCSIE 'Part 5: "Child-on-child sexual violence and sexual harassment" is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and do not dismiss it as banter (including bullying).
- Facilitate training and advice for all staff.

- all staff must read KCSIE Part 1 and all those working with children also Annex B
- Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the Board consider it will provide a better basis for those staff to promote the welfare and safeguard children.
- cascade knowledge of risks and opportunities throughout the organisation

Board of Directors/Safeguarding Link Director (Caroline Waldegrave)

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other directors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated – NB Safeguarding Training for school governors/Directors is free at safetraining.lgfl.net although at Leiths we use the NSPCC training.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions".
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Have regular strategic reviews with the online-safety coordinator (DSL) and incorporate online safety into standing discussions of safeguarding at board meetings.
- Work with the DSL and Principal to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B. This duty is overseen by the HR team as is all staff training.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.

Data Protection Officer (DPO) – Managing Director

Key responsibilities:

- Be aware that references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated

> Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The retention schedule for safeguarding records at Leiths is set at age 25.

- Work with the DSL, Principal and Board to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Students

Key responsibilities:

- Read, understand, sign and adhere to the guidelines in the Student Handbook with regard to acceptable use of online resources and systems and review this annually.
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the guidelines in the Student Handbook cover actions out of school, including on social media.

Appendix 2 – Related Policies and Documents

1. Safeguarding Concern log (Available to the Safeguarding Committee)
2. Safeguarding and Child Protection Policy
3. Student Handbook
4. Staff Code of Conduct
5. Online-Safety Questions from the Governing Board (UKCIS)
6. Working together to safeguard children (DfE)
7. Prevent Duty Guidance for Schools (DfE and Home Office documents)
8. Data protection policy