

Policy 3.7 – Learner E-Safety Policy

Policy Number	3.7	Review Cycle	3 Years	Reviewer
Date Created	January 2022	Review Date(s)		
Author	ICT and Data Manager			
Delegated Committee	Safeguarding, Prevent and Equalities			

This Policy should be read in conjunction with the following Landmarks policies and documents:

Policies	Documents
1.2 GDPR and Data Protection	Keeping Children Safe in Education
1.5 Anti-Bullying Policy	Department for Education: 'Preventing and Tackling Bullying'
1.6 Safeguarding Adults	Gov.uk: Searching, screening and confiscation
1.6a Safeguarding Children	Gov.uk: Prevent Duty Guidance
3.6 Positive Learning Support and Crisis Management	Education Act 2011
6.1 Digital Technology Acceptable Use	

All college policies are impact screened by the Safeguarding, Prevent and Equalities Committee (SPEC) when material changes are proposed to policies. It is for the Policy Author to highlight to SPEC when material changes are proposed.

The policy has been reviewed using the Equality Impact Screening tool (EIS), positive impact is explicitly intended and very likely.

This policy was externally reviewed by Jisc on 20th July 2022; recommendations have been implemented.

Policy 3.7 – Learner E-Safety Policy

Table of Contents

Scope and Purpose.....	2
The 4 Key Categories of Risk.....	2
Roles and Responsibilities.....	3
Educating Learners about Online Safety.....	4
Educating Parents/Carers about Online Safety.....	4
Cyberbullying.....	5
Examining Electronic Devices.....	5
Learners using Mobile Devices in College.....	5
Responding to Issues of Misuse.....	6
Monitoring Arrangements.....	6
3G/4G/5G Challenge.....	6
Annex 1 – Online Safety Concern Flowchart.....	7
Annex 2 – Accessible E-Safety Policy.....	8

Scope and Purpose

This policy is for use by all learners, staff members (including volunteers), and trustees of Landmarks. The college has a legal and professional obligation to safeguard its learners. This policy outlines:

- The robust processes that are in place to support learners to be safe online
- An overview of the different types of online safety concerns
- The preventative steps the college takes in promoting online safety
- The monitoring and reporting processes that are in place in relation to online safety

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk, as defined in Keeping Children Safe in Education (2022, paragraph 136):

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact** - being subjected to harmful online interaction with other users, such as online abuse and harassment, image-based abuse, peer-to-peer pressure,

Policy 3.7 – Learner E-Safety Policy

commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

Roles and Responsibilities

Board of Trustees:

- Landmarks' trustees are responsible for being aware of Landmarks' approach to online safety and hold the senior leadership team to account for its implementation.

Designated Safeguarding Lead (DSL):

- The DSL is responsible for working with the Principal, Designated Safeguarding Officers, the ICT and Data Manager, and other staff as necessary to address any online safety issues or incidents.
- Ensuring that any online safety incidents, including cyberbullying, are logged and dealt with appropriately.
- Liaising with other agencies and/or external services if necessary.

ICT and Data Manager:

- The ICT and Data Manager is responsible for ensuring an appropriate level of security protection procedures are in place, such as the college's filtering and monitoring system, NetSupport.
- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

All staff:

- All staff are responsible for following the college's safeguarding policies and procedures in relation to any online safety concerns.

Parents/Carers:

Policy 3.7 – Learner E-Safety Policy

- Notify the young person's personal tutor or a member of the safeguarding team if any concerns or queries are raised regarding e-safety.

Educating Learners about Online Safety

All learners will have different levels of understanding around the safe use of digital technology, so it is important that each individual's risk is detailed within their individual risk assessment; for example, some learners who are particularly vulnerable may require supervision when accessing college devices, while other learners will not.

The priority on education is to support learners to understand how to keep themselves safe online, including what to do if they find something worrying online.

Learners will be taught about online safety in a variety of ways, including:

- As part of the Personal and Social Development curriculum.
- Through RARPA targets, to support learners to work towards individualised online safety skills.
- The coverage of promotional events such as Safer Internet Day and Anti-Bullying Week.
- Individual information, advice and guidance.

Online safety topics will be delivered to learners depending on what is most relevant to them; for example, understanding the need to keep personal information private, knowing how to report concerns online, or the consequences of sharing inappropriate material.

Landmarks supports learners to self-refer concerns to the police where appropriate, or to report concerns on websites such as '[Report Harmful Content](#)'.

Educating Parents/Carers about Online Safety

The college will raise parent/carers' awareness of internet safety in communications home, and in information via our website or social media platforms. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their young person's personal tutor, who can provide information, advice and guidance about this topic.

Parents/carers can seek further guidance on keeping young people safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)



Policy 3.7 – Learner E-Safety Policy

- Talking to your child about online sexual harassment - [A guide for parents](#)

Cyberbullying

Cyberbullying is bullying which takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyberbullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The college will actively discuss cyberbullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

In relation to a specific incident of cyberbullying, the college will follow the processes set out in the college's anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among learners, the college will use all reasonable endeavors to ensure the incident is contained; the DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

College staff have the ability to search learners' electronic devices where they believe there is a good reason to do so, following the latest Department for Education guidance and practice. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the college rules

Learners using Mobile Devices in College

Learners may bring mobile devices into college, but are not permitted to use them during sessions unless directed to do so as part of a learning activity.

If using a mobile phone during sessions is becoming a distraction to learning, tutors may liaise with the learner and their support network to agree on the most suitable strategy moving forward – this could include a 'learner mobile phone contract' where the learner agrees to only use their phone during set times, or to hand in their phone at the start of the day, etc.



Policy 3.7 – Learner E-Safety Policy

Learners are expected to use the college's devices in line with its 'Digital Technology: Acceptable Use' policy.

Responding to Issues of Misuse

Where a learner misuses the college's ICT systems or internet, we will follow the procedures set out in the college's 'Digital Technology: Acceptable Use' policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. The college will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

See 'Annex 1' for the process detailing what happens when an e-safety concern is raised.

Monitoring Arrangements

Landmarks uses NetSupport as its filtering and monitoring software for college computers and laptops:

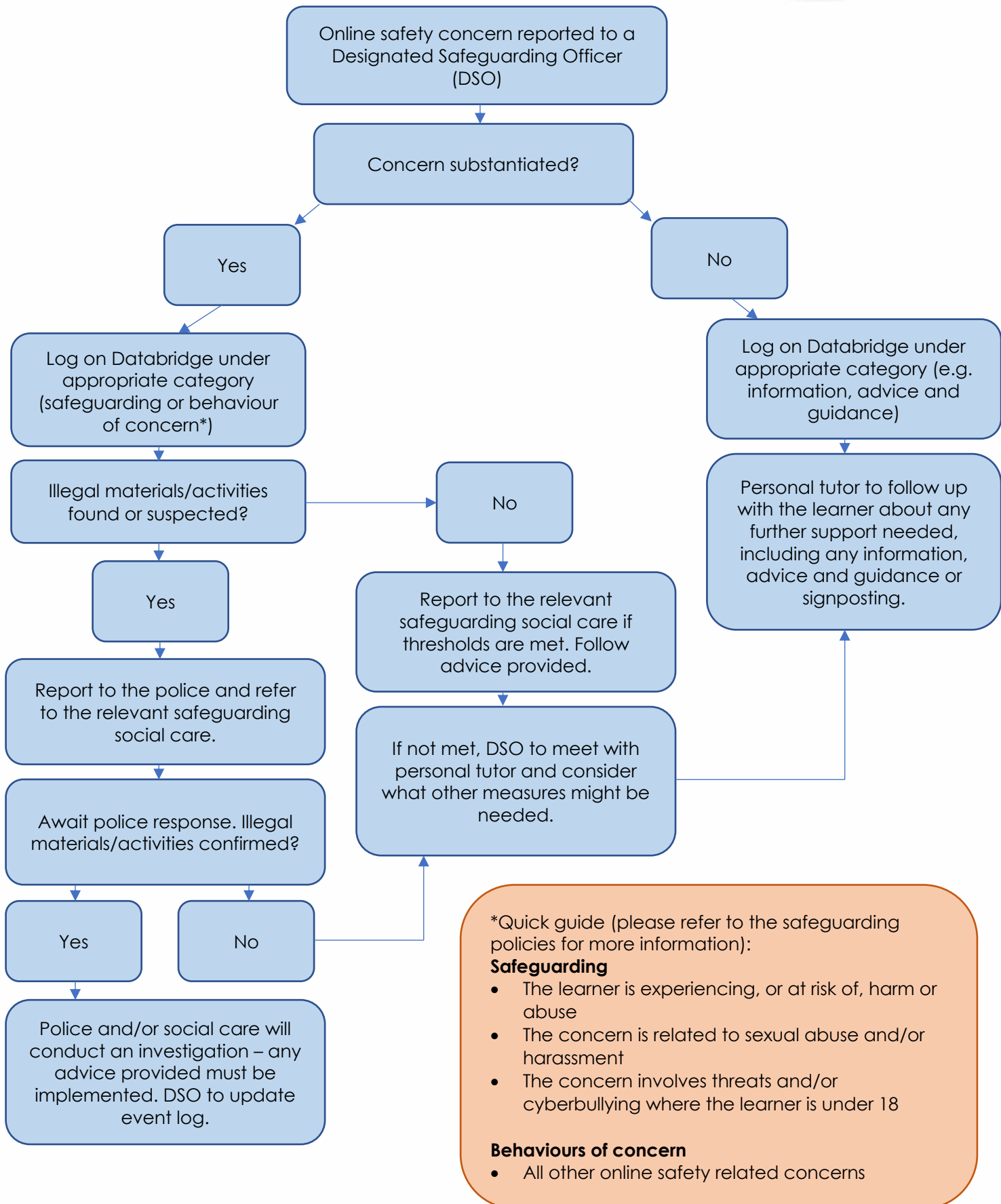
- NetSupport sends alerts to the DSL and ICT and Data Manager when a trigger word has been typed.
- If the alert is deemed to be a concern, the tutor of the session the learner is in will be contacted to intervene.
- The ICT and Data Manager is also able to remotely control learner laptops through NetSupport to close inappropriate material, if necessary.
- NetSupport alerts are monitored during fortnightly safeguarding meetings to ascertain any trends or concerning learner behaviour.
- NetSupport has the ability to block websites as required, though Landmarks' approach is to monitor and moderate rather than restrict access. Learners will be supported to understand the difference between appropriate and inappropriate websites to access at college.

3G/4G/5G Challenge

While the college uses NetSupport to monitor college devices, there is the ongoing challenge of learners being able to access the internet using mobile data, which cannot be monitored by the college. Landmarks also recognises that learners use the internet outside of college hours and cannot always be monitored. It is therefore increasingly important that learners understand how to keep themselves safe online and what to do if they ever feel unsafe online or worried about something they have seen (see Annex 2).



Policy 3.7 – Learner E-Safety Policy
Annex 1 - Online Safety Concern Flowchart





This policy explains how Landmarks will help you to keep safe online.



What is E-Safety?

	<p>E-Safety means 'staying safe online'.</p>
	<p>There are different types of risks online.</p>
What are the risks?	
	<p>Content: Being shown illegal, inappropriate, or harmful content.</p>
	<p>Illegal means against the law</p> <p>Inappropriate means it is bad to look at this</p>
	<p>This could include:</p> <ul style="list-style-type: none"> • pornography, • racism, • people being hurt, • people sharing extreme views.

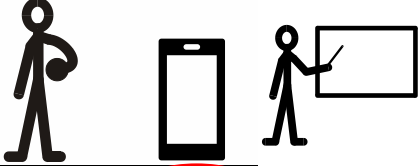

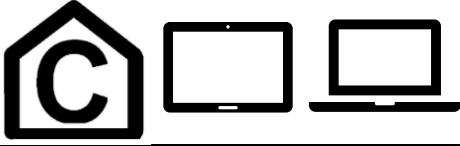






Policy 3.7 – Learner E-Safety Policy

	<p>Contact: Someone being mean to you online.</p>
	<p>This could include:</p> <ul style="list-style-type: none"> • online abuse, • bullying, • people pretending to be other people online.
	<p>Conduct: Behaviour online that could lead to harm.</p>
	<p>This could include: making, sending and receiving nude images, sharing nude images that have been sent to you.</p>
	<p>Commerce: Risks online that involve money.</p>
	<p>This could include:</p> <ul style="list-style-type: none"> • online gambling, • scams, • people trying to get your personal banking information.

Using Devices at College

	<p>Learners can use different devices at college.</p>
	<p>You could use your phone, an iPad, or a college laptop.</p>

Policy 3.7 – Learner E-Safety Policy

	<p>You can use your personal devices in sessions, if the tutor asks you to.</p>
	<p>You should not use your phone in sessions for anything else.</p>
	<p>You can use college devices like iPads and laptops in sessions or at break times.</p>
	<p>You must follow the rules when using college devices.</p>
	<p>This means you should not search for anything that could be inappropriate or illegal. (Look back at the risks online if you are not sure)</p>
	<p>Landmarks uses NetSupport to check what learners are looking at on college devices.</p>
	<p>If you search or type something inappropriate, staff will know.</p>
	<p>This is to make sure that everyone is safe.</p>
	<p>Staff might ask you about what you were looking at.</p>

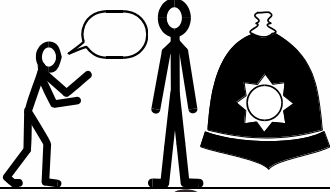
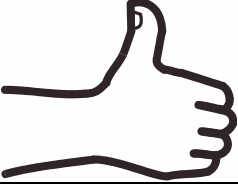
Policy 3.7 – Learner E-Safety Policy

	<p>If you keep looking at inappropriate content on college devices, you might not be allowed to use them anymore.</p>
--	---

Reporting Concerns

	<p>If you see something online that makes you feel unsafe or worried, there are different things you can do.</p>
	<p>If it happens at college, you can tell a member of staff.</p>
	<p>You could also click on the 'NetSupport' button.</p>
	<p>If it happens at home, you could tell a parent/carer.</p>
	<p>You could also report it online, using websites like 'Report Harmful Content'.</p>
	<p>Remember, you can always block people if they are posting things that you find worrying or upsetting.</p>
	<p>Telling someone is good.</p>

Policy 3.7 – Learner E-Safety Policy

	<p>We might need to tell someone else about your worry, like the police.</p>
	<p>This is okay!</p>

