| | |
|---|---|
| Title: | Safe use of the Internet Policy |
| Internal Reference: | L4L-GY - 010 |
| Approved by: | Sara Meller |
| Issue Date: | 22/08/2019 |
| Version No: | V1.a |
| Review Date: | 12/02/2025 |

Learning4Life-Gy CIC

# Safe use of the Internet Policy

## Scope of the Policy

This policy applies to all members of Learning4Life-GY including staff, students, volunteers, carers, visitors, who have access to and are users of Learning4Life-GY's digital technology systems.

# Directors

- The Directors have a duty of care for ensuring the safety (including online safety) of students of Learning4Life-GY, though the day to day responsibility for online safety will be delegated to the *Online Safety Officer.*
- The Directors should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

# Online Safety Officer

- leads the Online Safety
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with external technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- reports regularly to the directors

# Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters
- they report any suspected misuse or problem to the *Directors / Online Safety Officer* for investigation
- all digital communications with students / parents / carers should be on a professional level *and only carried out using official Learning4Life-GY Services systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Safe use of the Internet Policy
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

# Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

## Students:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the acceptable use of mobile phones.
- should understand the importance of adopting good online safety practice when using digital technologies.

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Learning4Life-GY will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and website. Parents and carers will be encouraged to support Learning4Life-GY in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Learning4Life-GY events
- their children's personal devices in Learning4Life-GY

# Policy Statements

## Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of Learning4Life-GY's online safety provision.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key online safety messages should be reinforced as part of a planned programme of tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

# Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Learning4Life-GY will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

# Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme.
- This Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Officer will provide advice / guidance / training to individuals as required.

# Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be owned by L4L-GY or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising Learning4Life-GY's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage.

All users should understand that the primary purpose of mobile / personal devices in a school context is educational.

# Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Learning4Life-GY will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Learning4Life-GY's equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or Learning4Life-GY into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission

## Communications

When using communication technologies, Learning4Life-GY considers the following as good practice:

- Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

# Social Media - Protecting Professional Identity

Learning4Life-GY has a duty of care to provide a safe learning environment for students and staff. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render Learning4Life-GY liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Learning4Life-GY provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils and staff through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Learning4Life-GY staff should ensure that:

- No reference should be made in social media to students, parents / carers or school / Learning4Life-GY staff
- They do not engage in online discussion on personal matters relating to members of the community
- Personal opinions should not be attributed to Learning4Life-GY
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with Learning4Life-GY or impacts on Learning4Life-GY, it must be made clear that the member of staff is not communicating on behalf of the service with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in Learning4Life-GY is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Learning4Life-GY permits reasonable and appropriate access to private social media sites

# Accessing and Posting material that encourages or endorses Terrorist acts

The Terrorism Act (2006) outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically.
Again, visits to websites related to jihadism and downloading of material issued by jihadist groups (even from open-access sites) may be subject to monitoring by the police.

# Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Learning4Life-GY and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. Learning4Life-GY believes that the activities referred to in the following section would be inappropriate and that users, as defined below, should not engage in these activities in / or outside the service when using Learning4Life-GY equipment or systems. Learning4Life-GY restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by  the school / academy | | | | | X | |

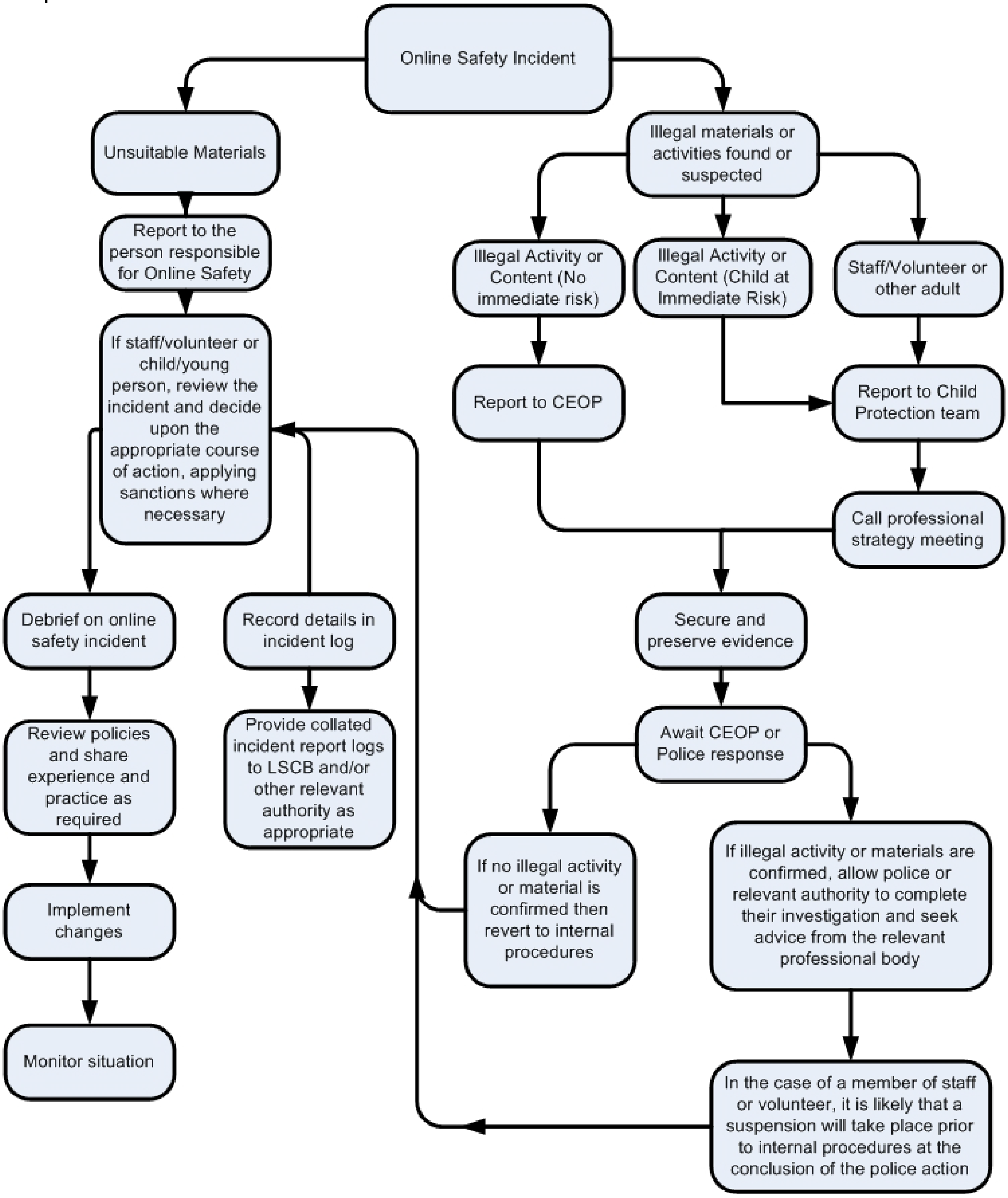
|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Infringing copyright |  |  |  | X |  |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) |  |  |  | X |  |
| Creating or propagating computer viruses or other harmful files |  |  |  | X |  |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) |  |  |  | X |  |
| On-line gaming (educational) | X |  |  |  |  |
| On-line gaming (non-educational) |  |  |  | X |  |
| On-line gambling |  |  |  | X |  |
| On-line shopping / commerce |  |  |  | X |  |
| File sharing |  |  |  | X |  |
| Use of social media |  | X |  |  |  |
| Use of messaging apps |  |  |  | X |  |
| Use of video broadcasting e.g. Youtube |  | X |  |  |  |

# Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

# Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

# Other Incidents

It is hoped that all members of Learjning4Life-GY will be responsible users of digital technologies, who understand and follow policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for Learning4Life-GY CIC and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

# Learning4Life-GY Actions & Sanctions

It is more likely that Learning4Life-GY will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

| Date | Changes Made | Signed |
|---|---|---|
| 12/02/24 | Added revision update table to end of policy. | Louis Meller |
| | | |
| | | |