**Gorse Hill Studios Creative Community**

**eSAFETY POLICY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Issue** | **Page(s)** | **Issue Date** | **Additions/Alterations** | **Initials** |
| 1 | All | July 2017 | All | JL  |
| 2 | All | July 2022 | All-update | LR |

**POLICY STATEMENT:**

Gorse Hill Studios is a charity youth organisation who set out to engage with young people and offer a place where they can express themselves freely within creative arts, these include:

* Music
* Drama
* Dance
* Art
* Digital Arts

GHS are aware that every young person has unique needs, but also accepts that everyone has the right to express themselves in a friendly, safe environment. Everyone involved in the organisation is required to read this policy carefully and read any future updates.

**Rationale**

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with children and young people are bound.

This policy applies to all members of GHS (including staff, volunteers, children and young people, parents / carers, visitors, partners, service users) who have access to and are users of communications technologies (whether these belong to the group or to the users themselves).

Digital technologies have become integral to the lives of children and young people in today’s society. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Children / young people, staff and volunteers have a right to safer internet access at all times.

However, the use of these new technologies can put users at risk. Some of the dangers may include:

* Access to illegal, harmful or inappropriate images or other content
* Loss of privacy / control of personal information
* Grooming by those with whom they make contact on the internet.
* The sharing / distribution of personal images without an individual’s consent or knowledge
* Inappropriate communication / contact with others, including strangers.
* Cyber-bullying
* Access to unsuitable video / internet games
* An inability to evaluate the quality, accuracy and relevance of information on the internet
* Plagiarism and copyright infringement
* Illegal downloading of music or video files
* Hacking, viruses and system security
* The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this esafety policy is used in conjunction with other policies (e.g., safeguarding policy).

As with all other risks, it is impossible to eliminate the risks completely. By providing good examples / role models and by raising awareness, it is possible to build the resilience of children and young people, so that they have the confidence and skills to deal with these risks.

Groups should be able to demonstrate that they have provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected to manage and reduce these risks. The information that follows explains how we intend to do this.

3

Gorse Hill Studios does not give out the WIFI information to children/young people, other than to staff, volunteers or session deliverers.

|  |  |
| --- | --- |
| **Should serious online incidents take place, the following external persons / agencies should be informed:**4 | **• GHS Safeguarding Lead** **• Local Authority Designated Officer (LADO) (if it involves an allegation against member of staff / volunteer) see Safeguarding Policy****• Police****• National / local organisation** |

**Online Safety Lead Person:**

8

The Online Safety Lead Person (session Leader):

* ensures that young people, staff / volunteers have an up-to-date awareness of the group’s current online safety policy and practices.
* ensures that all staff / volunteers are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* offers advice and support for all users.
* keeps up to date with developments in online safety.
* understands and knows where to obtain additional support and where to report issues.
* communicates with young people, parents and carers.
* records incidents.
* reports regularly to senior managers.

**Staff and volunteers**

are responsible for ensuring that:

**•** they have an up-to-date awareness of the group’s current online safety policy and practices.

• they report any suspected misuse or problem to senior managers, particularly where it is believed that a child’s welfare is at risk.

• digital communications with children and young people should be on a professional level

• young people in their sessions are aware of online safety.

• they are aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and handheld devices and that they monitor their use and implement the group policies with regard to these devices.

10

**Children and young people:**

* are expected to abide by the membership contract, which they will be expected to sign (depending on their age) before being given access to the organisation’s systems and devices.
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
* should demonstrate positive online behaviour.

**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.

* Parents / carers should sign the relevant permission forms on the taking and use of digital and video images.

**Policy Statements**

11

**Educating children and young people to stay safe online**

Whilst regulation and technical solutions are very important, their use should be balanced by making children and young people aware of the need to take a responsible approach to online safety. Children and young people need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

* Key online safety messages should be reinforced as part of all relevant planned programmes of activities for young people.
* Online safety issues should be discussed / highlighted, when possible, in informal conversations with young people.
* When the opportunity arises, young people should be advised to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information (not everything on the internet is true or accurate);
* Young people should be made aware of the need to respect copyright when using material accessed on the internet and, if applicable, acknowledge the source of information used.
* Staff and volunteers should act as good role models in their use of online technologies.

**Training – staff and volunteers**

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

* All staff will have access to a TES educare online training portal where there are multiple training modules, including -online safety
* The Safeguarding Lead will provide advice / guidance / training to individuals as required.

**Protecting the professional identity of staff and volunteers**

This applies to any adult, but particularly those working with children and young people (paid or unpaid) within the group. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the group.

Communication between adults and between children / young people and adults, by whatever method, should take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, webcams, websites and blogs.

**When using digital communications, staff and volunteers should:**

* only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the group.
* not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers;
* not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
* be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
* ensure that all communications are transparent and open to scrutiny.
* be careful in their communications with children so as to avoid any possible misinterpretation.

ensure that personal social networking profile details are not shared with children and young people (making every effort to keep personal and professional online lives separate)

not post information online that could bring the group into disrepute.

be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

E-mail, text or other web based communications between staff / volunteers and a child / young person should (wherever possible) take place using the group’s official equipment / systems.

Any communications outside the agreed protocols (above) may lead to disciplinary and/or criminal investigations.

**Wider personal use of digital communications:**

While the section above refers to communications between staff / volunteers and children / young people consideration should also be given to how the use of digital communications by staff and volunteers in their private lives could have an impact on the reputation of themselves and the group. Everyone should be able to enjoy the benefits of digital technologies. Staff and volunteers should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

* Careful consideration should be given as to who should be included as “friends” on social networking profiles and which information / photos are available to those friends.
* Privacy settings should be frequently reviewed.
* The amount of personal information visible to those on “friends” lists should be carefully managed and users should be aware that “friends” may still reveal or share this information.
* “Digital footprint” – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them.

Your technology

The group will be responsible for ensuring that all systems and devices will be as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Systems and devices will be managed in ways that ensure that the group meets accepted online safety requirements, as below:

* The use of the internet by children / young people must be supervised and / or monitored.
* Systems and devices will be regularly monitored.
* Personal data must not be sent over the internet or taken away from the group’s offices / facilities unless safely encrypted or otherwise secured;
* Passwords will be provided, where required, for those who need access to these systems / devices and access will be restricted for those who do not. Users will be required to change their password every term. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
* The “master / administrator” passwords for the systems / devices must be kept in a secure place by senior managers;
* Changes to systems and devices can only be made by those who have permission to do so e.g. installing software or changing security systems.

14

**How you use technology to communicate**

7

The following table shows how this group currently considers the benefit of using these technologies outweighs their risks / disadvantages:

|  |  |  |
| --- | --- | --- |
|   | **Staff & volunteers** | **Young people** |
| **Communication Technologies** | Allowed | Allowed at certain times | Allowed for selected staff / volunteers | Not allowed | Allowed | Allowed at certain times | Allowed with staff / volunteers permission | Not allowed |
| Mobile phones  |   |  **√** |   |   |   |  **√** |   |   |
| Taking photos on mobile phones or other camera devices |   |  **√** |   |   |   |  **√** |   |   |
| Use of hand held devices eg gaming consoles |   |  **√** |   |   |   |  **√** |   |   |
| Use of the organisation’s email for personal emails |   |  **√** |   |   |   |   |   |  **√** |
| Use of online communication technologies eg social networking, chat rooms, instant messaging, email |   |  **√** |   |   |   |  **√** |   |   |

When using communication technologies, GHScc considers the following as good practice:

* GHScc’s official email service may be regarded as safe and secure and is monitored.
* Users must immediately report to a senior manager the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication.
* Any communication between staff / volunteers and the children / young people or their parents / carers must be professional in tone and content. These communications should, where possible, only take place on official (monitored) systems.
* Young people should be taught about online safety issues, such as the risks attached to the use of personal details. They should also be informed of strategies to deal with inappropriate communications.
* Personal information should not be posted on the group website and, where possible, only official email addresses should be used to identify members of staff.

**Use of digital and video images**

7

The development of digital imaging technologies has created significant benefits, allowing users instant use of images that they have recorded themselves or downloaded from the internet. However, staff / volunteers and children / young people need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. GHSCC will raise awareness about these risks and will implement policies to reduce the likelihood of the potential for harm:

* When using digital images, staff and volunteers should raise awareness among children / young people 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.

15

* Permission from parents or carers will be obtained to allow images to be taken of their children / young people and also allowing their use for legitimate activities or for publicity that reasonably celebrates success and promotes the work of the group;
* Staff and volunteers are allowed to take digital / video images, where appropriate, but must check for permission concerning the sharing, distribution and publication of those images. Those images should be taken, where possible, on the organisation’s equipment, not the personal equipment of staff and volunteers.
* Care should be taken when taking digital / video images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the group into disrepute.
* Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images.
* The full names of young people will not be used anywhere on a website, blog, or published article, particularly in association with photographs unless consent is given. Consideration should be given to media coverage and journalists should be made aware of this policy.

**Unsuitable / inappropriate activities**

The group believes that the activities referred to in the following section would be inappropriate in a context of working with young people. The group policy restricts certain internet 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: 18 | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 |   |   |   |   | √ |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. |   |   |   |   | √ |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 |   |   |   |   | √ |
| 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  |   |   |   |   | √ |
| pornography |   |   |   | **√** |   |
| promotion of any kind of discrimination |   |   |   | **√** |   |
| threatening behaviour, including promotion of physical violence or mental harm  |   |   |   | **√** |   |
| any other information which may be offensive to colleagues or breaches the integrity of the ethos of the group or brings the group into disrepute |   |   |   | **√** |   |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards that are in place |   |   |   | **√** |   |
| Infringing copyright |   |   |   | **√** |   |
| Revealing or publicising confidential information (eg financial / personal information, computer / network access codes and passwords) |   |   |   | **√** |   |
| Creating or propagating computer viruses or other harmful files |   |   |   | **√** |   |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) |   |   |   | **√** |   |
| Using the group systems to run a private business |   |   |   |  **√** |   |
| On-line gaming (educational) |   |  **√** |   |   |   |
| On-line gaming (non educational) |   |   |   |  **√** |   |
| On-line gambling |   |   |   |  **√** |   |
| On-line shopping / commerce |   |  **√** |   |   |   |
| Downloading streaming illegal content |   |   |   |  **√** |   |
| File sharing (eg Bit Torrent, Limewire) |   |   |   |  **√** |   |
| Use of personal social networking sites(while "at work") |   |  **√** |   |   |   |
| Use of an official group social networking site |   |  **√** |   |   |   |
| Use of video broadcasting eg Youtube |   |  **√** |   |   |   |

**Sanctions Chart**

If staff / volunteers suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that a senior manager is informed.

It is intended that incidents of misuse will be dealt with through any accepted disciplinary procedures as follows:

20

|  |
| --- |
| Young People |
| Incidents: | Refer to Leader | Refer to Police | Requires technical response / support  | Inform parents / carers | Removal of access to technology / devices  | Warning | *Further sanction (to be described)*  |
| Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities). | **√** | **√** | **√** | **√** | **√** | **√** |  |
| Unauthorised downloading or uploading | **√** |  | **√** | **√** | **√** | **√** |  |
| Allowing others to access technology / devices by sharing username and passwords | **√** |  |  |  |  |  |  |
| Attempting to access or accessing the technology / devices, using another person’s account (hacking) | **√** |  |  | **√** | **√** | **√** |  |
| Corrupting or destroying the data of other users | **√** |  |  | **√** | **√** | **√** |  |
| Sending a communication that is regarded as offensive, harassment or of a bullying nature | **√** |  |  | **√** | **√** | **√** |  |
| Actions which could bring the organisation into disrepute.  | **√** |  |  | **√** | **√** | **√** |  |
| Deliberately accessing materials that the group has agreed is inappropriate | **√** |  |  | **√** | **√** | **√** |  |
| Activities that infringe copyright or data protection.21 | **√** |  |  | **√** | **√** | **√** |  |
| Using proxy by-pass sites or other means to subvert the filtering system | **√** |  |  | **√** | **√** | **√** |  |
| Accidentally accessing materials that the group has agreed is inappropriate and failing to report it. | **√** |  |  | **√** | **√** |  |  |
| Unauthorised use of mobile phone / digital camera / other handheld device | **√** |  |  |  |  |  |  |
| Unauthorised use of social networking / instant messaging / personal email | **√** |  |  |  |  |  |  |

|  |
| --- |
| Staff and volunteers  |
| Incidents: | Refer to line manager / Leader | Refer to National / Local Organisation / body  | Refer to Police | Requires technical response / support | Warning | Suspension | Disciplinary action |
| Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities). | **√** | **√** | **√** |  |  |  |  |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email "while at work" | **√** |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files | **√** |  |  |  |  |  |  |
| Disclosing passwords or any information relating to the security of technology and devices.  | **√** |  |  |  |  |  |  |
| Accidental infringement of the organisation’s personal data policy | **√** |  |  |  |  |  |  |
| Deliberate infringement of the organisation’s personal data policy | **√** |  |  |  | **√** |  |  |
| Corrupting or destroying the data of other users  | **√** |  |  |  |  |  |  |
| Deliberate damage to hardware or software | **√** |  |  |  | **√** | **√** |  |
| Sending a communication that is offensive, harassment or of a bullying nature | **√** |  |  |  | **√** | **√** | **√** |
| Using personal communication technologies eg email / social networking / instant messaging / text messaging to communicate with young people (except where allowed in the policy) | **√** |  |  |  | **√** |  |  |
| Actions which could compromise the professional integrity of staff / volunteers | **√** |  |  |  |  |  |  |
| Bringing the organisation into disrepute | **√** |  |  |  | **√** |  | **√** |
| Deliberately accessing materials that the group has agreed is inappropriate | **√** |  |  |  | **√** | **√** | **√** |
| Breaching copyright or licensing regulations | **√** |  |  |  | **√** | **√** | **√** |
| Using proxy by-pass sites or other means to subvert the filtering system | **√** |  |  |  |  |  |  |
| Accidentally accessing materials that the group has agreed is inappropriate and failing to report it. | **√** |  |  |  |  |  |  |

**Flowchart for responding to online safety incidents**



**Supporting Policies**

23

23

**On the following pages you will find a range of supporting policies:**

**Management:**

1. Template acceptable use policy for children and young people (older children)
2. Template acceptable use policy for young children (eg age 8 or younger)
3. Template accptable use policy for staff and volunteers (including professional identity)
4. Template consent form for parents and carers (including use of images)
5. Template personal data policy

**People:**

1. Flowchart for responding to online safety incidents
2. Guidance for reviewing internet sites (for suspected harassment and distress)
3. Template reporting log
4. Template training needs audit

**Technology**

1. Template password security policy
2. Template monitoring log

**At the end of this document you will find:**

**Links to other organisations and documents**

**Legislation**

**Glossary**

**Acknowledgements**

**Acceptable Use Policy**

7

**Acceptable Use Policy Agreement**

I understand that while I am a member of Gorse Hill Studios, I must use technology in a responsible way.

**For my own personal safety:**

• I understand that my use of technology will be supervised and monitored.

• I will keep my password safe and will not use anyone else’s (even with their permission)

• I will keep my own personal information safe as well as that of others.

• I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

**For the safety of others:**

25

• I will not interfere with the way that others use their technology.

• I will be polite and responsible when I communicate with others,

• I will not take or share images of anyone without their permission.

**For the safety of the group:**

 • I will not try to access anything illegal

• I will not download anything that I do not have the right to use.

• I will only use my personal device if I have permission and use it within the agreed rules

• I will not deliberately bypass any systems designed to keep GHSCC safer.

• I will tell a responsible person if I find any damage or faults with technology, however this may have happened.

• I will not attempt to install programmes of any type on the devices belonging to GHSCC, without permission.

• I will only use social networking, gaming, and chat sites with permission

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

26

***Name***

***Signature***

***Date***

**Acceptable Use Agreement for Staff and Volunteers**

7

**Background**

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

* Staff and volunteers will act responsibly to stay safer while online, being a good role model for younger users.
* effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
* staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term “professional” is used to describe the role of any member of staff, volunteer or responsible adult.

**For my professional and personal safety I understand that:**

* I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring my group into disrepute.
* My use of technology could be monitored.
* When communicating professionally I will use the technology provided by GHSCC (e.g. email). (You should amend this section to take account of your policy on communications with children / young people and parents / carers. Staff and volunteers should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications).
* These rules also apply when using GHSCC’s technology either at home or away from GHSCC site.
* Personal use of GHSCC’s technology is only acceptable with permission.

**For the safety of others:**

* I will not access, copy, remove or otherwise alter any other user’s files, without authorisation.
* I will communicate with others in a professional manner.
* I will share other’s personal data only with their permission.
* I understand that any images I publish will be with the owner’s permission and follow the group’s code of practice.
* Wherever possible I will use the group’s equipment to record any digital and video images, unless I have permission to do otherwise.

**For the safety of the group, I understand that:**

* I will not try to access anything illegal, harmful or inappropriate.

28

* It is my responsibility to immediately report any illegal, harmful or inappropriate incident.
* I will not share my online personal information (eg social networking profiles) with the children and young people in my care.
* I will not deliberately bypass any systems designed to keep GHSCC safer.

29

* I will only transport, hold, disclose or share personal information about myself or others, as outlined in the confidentiality policy. Where personal data is transferred, externally, it must be encrypted.
* I understand that data protection policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the organisation’s policy to disclose such information to an appropriate authority.
* Personal passwords and those of other users should always be confidential.
* I will not download anything that I do not have the right to use.
* I will only use my personal device if I have permission and use it within the agreed rules
* I will inform the appropriate person if I find any damage or faults with technology.
* I will not attempt to install programmes of any type on the devices belonging to GHSCC, without permission.

**Staff / Volunteer Name**

**Signed**

**Date**

29

Use of Digital / Video Images

The use of digital / video images plays an important part in our activities. Children / young people, staff and volunteers may use digital cameras or other devices to record evidence of those activities. These images may then be used in Learning Journeys and presentations and may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media.

The group will comply with the Data Protection Act and request parents / carers permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

*It’s a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping our children safe by considering the following:*

* *Images and video should be for your own or family’s personal use only*
* *Think about privacy and who has the right to see your images, not only of your own child but of others*
* *If you do share the images online, then you must make sure they are limited to immediate family only and not public*
* *If you need help in knowing how to do this then come and have a chat with us*

Parents / carers are requested to sign the permission form below to allow the group to take and use images of their children.

Permission Form

**Parent / Carers Name**

**Name of Child / Young Person**

As the parent / carer of the above child, I agree to the group taking and using digital / video images of my child / children. I understand that the images will only be used to support legitimate activities or in publicity that reasonably celebrates success and promotes the work of the group.

I agree that if I take digital or video images at group events which include images of children, other than my own, I will abide by these guidelines in my use of the images.

**Signed Date**

**Flowchart for responding to online safety incidents**



**Guidance for Reviewing Internet Sites (for suspected harassment and distress)**

This guidance is intended for use when groups 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 typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking, messaging sites, gaming sites or blogs etc.

**Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police.**

**Please follow all steps in this procedure:**

* Have more than one senior member of staff / volunteer 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 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

* **Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

**Record of reviewing internet sites (for suspected harassment / distress)**

|  |  |
| --- | --- |
| Group |  |
| Date |  |
| Reason for investigation |  |

**Details of first reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

**Details of second reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

**Name and location of computer used for review**

|  |
| --- |
|  |

**Web site(s) address Reason for concern**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

**Conclusion and Action proposed or taken**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Reporting Log**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Reporting LogGroup .............................................................. | Signature |  |  |  |  |  |  |  |  |
| Incident Reported by |  |  |  |  |  |  |  |  |
| Action taken | By whom? |  |  |  |  |  |  |  |  |
| What? |  |  |  |  |  |  |  |  |
| Incident |  |  |  |  |  |  |  |  |
| Time |  |  |  |  |  |  |  |  |
| Date |  |  |  |  |  |  |  |  |

**Password Security Policy**

**Introduction**

GHSCC will be responsible for ensuring that the technologyis as safe and secure as is reasonably possible and that:

* users can only access data to which they have permission.
* access to personal data is securely controlled in line with the group’s personal data policy

**Responsibilities**

* **Each user (adults and young people) should have their own password and be responsible for it’s security.**
* *Passwords for new users, and replacement passwords for existing users will be allocated by administrator (Caroline Gleaves or Louise Russell).*
* *Users will change their passwords every at least every term.*

**Training / Awareness**

* It is essential that users should be made aware of the need for keeping passwords secure.
* Adult users will be made aware of the password policy:

- at induction

- through the Acceptable Use Agreement

* Children / young people will be made aware of the password policy:

 - when joining the group

 - informally through reminders from staff / volunteers

 - through the Acceptable Use Agreement

35

**Policy Statements**

All users will be provided with a username and password by Louise Russell/Caroline Gleaves who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

*•* **the “master / administrator” passwords for GHSCC should be held by more than one person (including the senior leader), should not be used for day to day use and must be stored securely.**

*• passwords must be changed every term*

*• the password should fit with the programmes requirements:*

*• should include a mixture of types of character*

*• should not include names*

*• temporary passwords e.g. users with new user accounts or replacement passwords will be forced to change the temporary password when they next log-on*

*• there should be an agreed system for requests for password changes.*

Where sensitive data is in use (particularly if accessed on laptops) GHSCC may require adult users to use more secure forms of authentication e.g. two factor authentication.

**Links to other organisations or documents**

**The following sites will be useful as general reference sites, many providing good links to other sites:**

South West Grid for Learning: **www.swgfl.org.uk/safe**

Childnet: **www.childnet.com**

CEOP - Think U Know: **www.thinkuknow.co.uk**

Netsmartz: **www.netsmartz.org**

Teach Today: **www.teachtoday.eu**

Internet Watch Foundation (report criminal content): **www.iwf.org.uk**

UK Council for Child Internet Safety: **www.education.gov.uk/ukccis**

Safer Internet Centre: **www.saferinternet.org.uk**

**Management**

Online Compass. This is for groups that work with children and young people – this self review tool allows groups that work with children to assess their policy and provision. **www.onlinecompass.org.uk**

SWGfL School E-Safety Policy Templates: **www.swgfl.org.uk/esafetypolicy**

Plymouth Early Years E-Safety Toolkit: **www.plymouth.gov.uk/early\_years\_toolkit.pdf**

Byron Review(“Safer Children in a Digital World”) **http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/**

Guidance for safer working practice for adults that work with children and young people - [**http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/**](http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/)

The Learning Trust Example Online Safety Policy (Schools): [**http://trustnet.learningtrust.co.uk/Trust/forms/ICT/ICT%20Policies/Internet%20Safety%20Policy.pdf**](http://trustnet.learningtrust.co.uk/Trust/forms/ICT/ICT%20Policies/Internet%20Safety%20Policy.pdf)

Belfast Computer Clubhouse Example:

[**http://www.belfastclubhouse.org/word/Membership-Form.doc**](http://www.belfastclubhouse.org/word/Membership-Form.doc)

Tech Mission Safe Families AUP: **www.safefamilies.org/aup**

Policies for voluntary groups eg Woodcraft Folk: **www.woodcraft.org.uk/safeguarding**

Somerset e-sense progression (e-safety curriculum): [**https://slp.somerset.gov.uk/cypd/elim/somersetict/Site%20Pages/Progressions%20-%20eSense.aspx**](https://slp.somerset.gov.uk/cypd/elim/somersetict/Site%20Pages/Progressions%20-%20eSense.aspx)

Ofsted survey: **www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB**

Protecting your personal information online: **www.ico.gov.uk/~/media/documents/library/data\_protection/practical\_application/protecting\_your\_personal\_information\_online.ashx**

Getnetwise privacy guidance: [**http://privacy.getnetwise.org/**](http://privacy.getnetwise.org/)

**People**

CBBC (stay safe): **www.bbc.co.uk/cbbc/help/home**

Oldham LSCB Youth Council Charter of Young Peoples Digital Rights: **www.esafetyweek.info**

NSPCC: **www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety\_wdh72864.html**

Vodafone Parents Guide: [**http://parents.vodafone.com**/](http://parents.vodafone.com/)

Google guidance for parents: **www.teachparentstech.org**

E-Parenting tutorials: [**http://media-wareness.ca/english/parents/internet/eparenting.cfm**](http://media-awareness.ca/english/parents/internet/eparenting.cfm)

Training - SWGfL EPICT: **www.swgfl.org.uk/Epict**

Training - SQA Internet Safety qualification: **www.sqa.org.uk/sqa/34591.html**

Practical Participation – Tim Davies: **www.practicalparticipation.co.uk/yes/**

Protecting Professional Identity documents: [**http://public.merlin.swgfl.org.uk/establishments/879/PlymouthChildrensServicesICTAdvice/Pages/ProtectingYourProfessionalIdentity.aspx**](http://public.merlin.swgfl.org.uk/establishments/879/PlymouthChildrensServicesICTAdvice/Pages/ProtectingYourProfessionalIdentity.aspx)

SWGfL Facebook Checklist:

**www.swgfl.org.uk/FacebookChecklist**

Digital Citizenship: **www.digizen.org.uk**

Kent “Safer Practice with Technology”: [**http://kentrustweb.org.uk/CS/community/kent\_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx**](http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx)

Connect Safely Parents Guide to Facebook:

**www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html**

Ofcom – Help your children to manage the media: [**http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/**](http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/)

Mobile broadband guidance: **www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/**

Orange Parents Guide to the Internet: **www.orange.co.uk/communicate/safety/10948.htm**

O2 Parents Guide: **www.o2.co.uk/parents**

FOSI – Family Online Internet Safety Contract: **www.fosi.org/resources/257-fosi-safety-contract.html**

Office for Internet Safety (Ireland) – guide for parents: **www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-guideparents-en**

Cybermentors (Beat Bullying): **www.cybermentors.org.uk**

Teachernet Cyberbullying guidance:

www.digizen.org/resources/cyberbullying/overview

“Safe to Learn – embedding anti-bullying work in schools”

www.anti-bullyingalliance.org.uk/tackling\_bullying\_behaviour/in\_schools/law,\_policy\_and\_guidance/safe\_to\_learn.aspx

Anti-Bullying Network: **www.antibullying.net/cyberbullying1**

Cyberbullying.org: **www.cyberbullying.org**

**Technology**

Kaspersky – advice on keeping children safe: **www.kaspersky.co.uk/keeping\_children\_safe**

Kaspersky - password advice: [**www.kaspersky.co.uk/passwords**](http://www.kaspersky.co.uk/passwords)

CEOP Report abuse button: **www.ceop.police.uk/Safer-By-Design/Report-abuse/**

**Legislation**

Groups should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

**Computer Misuse Act 1990:**

This Act makes it an offence to:

• Erase or amend data or programs without authority;

• Obtain unauthorised access to a computer;

• “Eavesdrop” on a computer;

• Make unauthorised use of computer time or facilities;

• Maliciously corrupt or erase data or programs;

• Deny access to authorised users.

**Data Protection Act 1998**

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed.

• Processed for limited purposes.

• Adequate, relevant and not excessive.

• Accurate.

• Not kept longer than necessary.

• Processed in accordance with the data subject’s rights.

• Secure.

• Not transferred to other countries without adequate protection.

**Freedom of Information Act 2000**

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**

49

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

• Establish the facts;

• Ascertain compliance with regulatory or self-regulatory practices or procedures;

• Demonstrate standards, which are or ought to be achieved by persons using the system;

• Investigate or detect unauthorised use of the communications system;

• Prevent or detect crime or in the interests of national security;

• Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:

• Ascertain whether the communication is business or personal;

• Protect or support help line staff.

• The school reserves the right to monitor its systems and communications in line with its rights under this act.

**Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

**Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

**Telecommunications Act 1984**

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

**Criminal Justice & Public Order Act 1994**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

**Racial and Religious Hatred Act 2006**

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

50

**Protection from Harrassment Act 1997**

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

**Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

**Sexual Offences Act 2003**

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

**Public Order Act 1986**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

**Obscene Publications Act 1959 and 1964**

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

**Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the context of work with young people, human rights to be aware of include:

• The right to a fair trial

• The right to respect for private and family life, home and correspondence

• Freedom of thought, conscience and religion

• Freedom of expression

• Freedom of assembly

• Prohibition of discrimination

• The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

52