Castlebar School
Online Safety Policy

Contents

1. Introduction

Computing is an essential resource to support learning and teaching and has an important everyday role in children's lives. We therefore need to build the use of Computing/ ICT to give them skills to access life-long learning.

Computing covers a wide range of resources including; web-based and mobile learning. There is constant evolution of computing and technology within society. Currently the internet technologies children and young people are using both inside and outside of the classroom could include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking, Blogs and Wikis, Podcasting
- Video Broadcasting and live streaming
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial much technology, particularly web-based resources, is not consistently policed. All need to be aware of the range of risks linked with the use of Internet technologies.

At Castlebar, we understand the responsibility to educate pupils on online safety issues; teaching appropriate behaviours to enable them to remain safe and legal when using the internet and related technologies, in and beyond the classroom.

This policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, Smartphones, etc.); and technologies owned by pupils, staff and governors, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc.).

2. Pupils with additional needs

At Castlebar we cater for pupils who require additional specialist teaching and differentiated curriculum in order to address learning and communication difficulties. This means that we need to be even more vigilant to address issues of online safety at a level that they can understand including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

For our pupils with difficulties in social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned, well managed and supervised for these children and young people.

We understand that there is an associated further vulnerability for our pupils when interacting with internet technologies therefore ensure our practice safety standards are of very high quality.

3. Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Online safety issues at Castlebar are dealt with as child protection problems which are addressed by the Child Protection Lead Officer: Paul Adair and the Safeguarding team. All members of the school community are made aware of this. The role of the Safeguarding Team is to keep abreast of current issues and guidance.

Senior Management and Governors are to be updated by the Head/ Safeguarding Team in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community in accordance with 'Keeping Children safe in education' (Sept 2016)

Online safety skills development for staff

- Staff will receive regular information and training on online safety issues as part of the ongoing CPD training.
- New staff will receive the school's Acceptable Use Agreement as part of induction.
- All staff will be made aware of individual safeguarding responsibilities relating to online safety and know what to do in the event of misuse of technology (see attached flowchart).
- All staff are to incorporate online safety activities and awareness within their curriculum areas.

Managing the school online safety messages

- We endeavour to embed online safety messages whenever the internet and/or related technologies are used.
- The online safety policy, at a level appropriate to the understanding of the children, will be introduced to the pupils at the start of each school year.
- Online safety posters will be prominently displayed.
- The school uses online safety and Security software.

4. Online safety in the Curriculum

Computing and online resources are increasingly used across the curriculum it is therefore essential for online safety guidance to be given to the pupils on a regular basis.

- The school provides opportunities in a range of curriculum areas to teach online safety.
- Educating pupils on the dangers of technologies encountered outside school is done informally when opportunities arise.
- Adults are aware of relevant legislation on using internet such as data protection and intellectual property which may limit what they want to do but serves to protect. This is presented, where deemed appropriate, at the pupils' level of understanding.
- Pupils are taught about respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils will be made aware, if appropriate and at a suitable level of understanding, of the impact of online bullying. Parents will be given the opportunity to take part in workshops outlining the characteristics of cyber bullying and know how to seek advice or help if their child experiences problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as ChildLine/ CEOP report abuse button.
- Staff are taught to critically evaluate materials and teach good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- Web filtering is controlled by LGfL which denies access to inappropriate/illegal websites, which may contain images of a sexual nature or extreme views. (Radicalisation).

5. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared. Pupils/ Parents are expected to keep any passwords secret and not to share with others. Staff and pupils will be regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement.
- Staff are provided with Military strength Encrypted USB device.
- If you think a password may have been compromised report this to the Computing TLR or the IT
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform. Individual staff users must also make sure that workstations are not left unattended and are locked.

6. Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.
The school follows Becta guidelines in accordance with GDPR recent changes.

- Staff and governors are aware of their responsibility when accessing school data. Level of access is determined by the Headteacher.
- Any data taken off the school premises must be encrypted, on a provided encrypted USB device.
- The school network is back up internally / using a secure remote back up facility.
- Staff are made aware of this through regular training and online safety training.
- Selected Staff and Governors are provided with OTP tags to access important/delicate information.

7. Managing the Internet

The internet is an open communication medium. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource but also a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- The school maintains that pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure
- School internet access is controlled by LGfL web filtering which denies access to inappropriate websites including pornography, radicalisation and extremist views.
- Castlebar School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the online safety co-ordinator. The offending URL will be reported to the LA and LGfL.
- Sophos Anti-Virus protection is set to automatically update on all school machines with access to the internet.
- In addition staff laptops used at home can also be protected by Sophos Anti-Virus.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

8. Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly within education, can provide easy to use, creative, collaborative and free facilities. It is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our staff acting on behalf of our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- We endeavour to deny access to social networking sites to pupils within school.
- All pupils, and in loco parentis, staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- There is no placing of pupil images (or details within images that could give background details) on such sites.

- No pupil's personal details are given out on such sites which may identify them or where they are.
- Our pupils and staff who monitor all internet activity are to report any incidents.
- Pupils are to be introduced to Web2 tools within the safe context of LGfL MyUSO.
- Staff understand it is highly inappropriate to use open social networking sites and public chat room facilities with pupils. They are expected to use the tools within the resources provided.

9. Mobile technologies

Emerging technologies may offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Existing mobile technologies such as tablets, portable media players, PDAs, gaming devices, mobile and Smartphones are familiar to children outside of school too. There is risk and misuse associated with communication and internet use therefore technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.
Mobile devices (including phones)
- The school allows staff to bring in personal mobile phones and devices for their own use.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Technology may be used, for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

10.   Managing email

The use of email within school is an essential means of communication. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that our pupils need 1:1 support, guidance and approval IF email is to be used on their behalf.
- Staff have a school LGfL account for all school business to minimise risk of receiving unsolicited or malicious emails and avoid personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use school approved accounts (LGfL LondonStaffMail) on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are to adhere to the accepted rules of network etiquette (netiquette) particularly in relation to use of appropriate language and not revealing any personal details about themselves or others, or arrange to meet anyone without specific permission.
- Pupils, or staff monitoring email use, must immediately report any offensive message and keep the offending message(s) as evidence.
- Staff must inform the online safety co-ordinator if they receive an offensive e-mail.

11.   Safe Use of Images / Film

Taking of Images and Film
Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Photos and videos are used as a means of assessment at Castlebar and it is the responsibility of all staff to ensure these images are safely secured.

Consent of adults who work at the school
- Permission to use images of all staff who work at the school is sought on a regular basis.
- Statement of agreement from parents: I agree that any photographs or images taken at school events are for personal use only and will not be used in social media or on the internet.
- Parents are requested NOT to video school performances. Video are captured ONLY by school staff.

Publishing pupil's images and work
On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:
- On the school web site/ on line
- In the school prospectus and or publications that may produce for school promotion
- Recorded/ transmitted on a video or webcam
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/ carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Video is only streamed from the service set to private. Only the Web Manager has authority to upload to the public website.

Storage of Images
- Images/ films of children are to only be stored on the school's network and encrypted mobile storage devices and should be removed from the class camera.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- Staff have the responsibility of deleting images when no longer required.

Webcams and CCTV
- The school uses CCTV for security and safety. This is only accessed by authorised staff. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school other than for special specifically vetted and authorised projects. Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document).
- Consent is sought from parents/carers and staff on joining the school, as for all images.

Video Conferencing
- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff if video conferencing
- Approval from the Headteacher is sought prior to all video conferences within school.

Visitors to Castlebar
- All persons who enter Castlebar School staff, parents or visitors are bound by the Acceptable User Policy. This policy clearly outlines the use of recordings.
- No images of pupils are to be uploaded to social networking sites, without first receiving written permission from parents/carers.

12.   Misuse and Infringements

Complaints
Complaints relating to online safety should be made to the online safety co-ordinator or Headteacher.
Incidents should be logged (see Incident Log in Appendix) and process should be followed (see Flowchart in Appendix E).

Inappropriate material
- All users must be aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online safety co-ordinator.
- Deliberate access to inappropriate materials by anyone will lead to the incident being logged by the online safety co-ordinator and, depending on the seriousness of the offence; investigation by the Headteacher and Local Authority and immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

13.   Equal Opportunities

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules.

14.   Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting online safety both in and outside of school.   We aim to regularly consult and discuss online safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.
- Parents/ carers and pupils are to be actively encouraged to contribute to adjustments or reviews of the school online safety policy.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to online safety where appropriate in the form of;
  - Information meetings/Parental workshops
  - Posters
  - Website/ Learning Platform training and postings
  - Newsletter items

15.   Current Legislation

Acts relating to monitoring of staff email
Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are

relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998, http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to online safety

Racial and Religious Hatred Act 2006
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.

Sexual Offences Act 2003
The new grooming offence 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.   Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)
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.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:
- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
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.

Protection of Children Act 1978 (Section 1)
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.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment 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.

Counter terrorism and security Act 2015
In July 2015 the UK Government published the following document with advice for schools about how the new law impacts on schools' duty under the 'Prevent' scheme. This was aimed at Safeguarding children against Radicalisation. A school-specific section can be found on pages 10-13.
https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

16.   Review Procedure

There will be an on-going opportunity for staff to discuss with the online safety coordinator any issue of online safety that concerns them. The process of reporting incidents is ingrained within the practice of the school and is annually addressed through staff CPD training.
This policy will be reviewed regularly and consideration given to the implications for future whole school development planning.
The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. In accordance with recognised best practice this policy will be reviewed on a regular basis in line with safeguarding policy procedures.

Castlebar School   May 2018

RATIFIED BY THE GOVERNING BODY ON: 11th May 2018   REVIEW DATE: 2021

APPENDIX A: Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT both in school and in a professional capacity outside school e.g. trips, residential outings.

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Alan Guy, school online safety coordinator.

➢ I will only use the school's email / Internet / Intranet / MLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
➢ I will comply with the ICT system security and not disclose to other individuals any passwords provided to me by the school or other related authorities.
➢ I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
➢ I will only use the approved, secure email system(s) and MLE tools for communications with pupils / students / parents.
➢ I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter in this school.
➢ I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be accessed remotely when authorised by the Head or Governing Body using the secure systems implemented.
➢ I will not install any hardware or software without permission of the network manager.
➢ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory and **understand that to do so may constitute a disciplinary offence and in some cases a criminal offence.**
➢ Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
➢ I will respect copyright and intellectual property rights.
➢ I will ensure that my online activity, both in school and outside school, will not bring the school or my professional role into disrepute.
➢ I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ………………………….………… Date ……………………

Full Name ……………………………………….. (printed)

Job title ……………………………………………………………………………

APPENDIX B: Castlebar School Acceptable ICT Use Agreement: Pupils

I will……

Use technology for school work only.

Not tell other people my passwords.

Not use other people's passwords.

Will tell my teacher if I find/see bad things.

Will not give out my details to people I meet online.

## APPENDIX C: Castlebar School Acceptable ICT Use Agreement: Parents

Dear Parent/ Carer
        ICT including the internet, email and mobile technologies, etc. has become an important part of learning our school. We will work with the school to keep children safe and help them to learn responsible and respect use of technology.
Please read and discuss these online safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Alan Guy.

✂ ………

Parent/ carer signature

We have discussed this and …………………………………..........(child name) agrees

to follow the online safety rules and to support

to the safe use of technology both at Castlebar School and outside school.

Parent/ Carer Signature …….………………….………………………….

Class ………………………………… Date ………………………………

APPENDIX D: Incident Log

Castlebar School online safety Incident Log Sheet
Details of all online safety incidents are to be reported to the online safety co-ordinator. Incident Log Sheets will be added to an Incident Log File which will be monitored by the Headteacher, Member of SLT or Chair of Governors.
NOTE:

- Any incidents that involve child protection issues need to be brought to the immediate attention of the Child Protection officer including incidents of extremism or suspected sexting.
- Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	M/F	Room & ICT device (number if possible)	Details of incident (including evidence)	Actions & reasons

APPENDIX D: Incident Log

APPENDIX E: Flowchart for Misuse/Infringements

```
                              Online Safety Incident

        Unsuitable Materials                    Illegal materials or
                                                activities found or
                                                     suspected

        Report to the
     person responsible          Illegal Activity or    Illegal Activity or     Staff/Volunteer or
     for Online Safety           Content (No            Content (Child at        other adult
                                 immediate risk)        Immediate Risk)

     If staff/volunteer or
        child/young                                                             Report to Child
     person, review the          Report to CEOP                                 Protection team
     incident and decide
           upon the
     appropriate course
     of action, applying                                                       Call professional
      sanctions where                                                          strategy meeting
         necessary

     Debrief on online      Record details in            Secure and
     safety incident        incident log              preserve evidence

     Review policies      Provide collated            Await CEOP or
     and share            incident report logs        Police response
     experience and       to LSCB and/or
     practice as          other relevant
     required             authority as            If no illegal activity     If illegal activity or materials are
                          appropriate             or material is             confirmed, allow police or
                                                  confirmed then             relevant authority to complete
       Implement                                  revert to internal         their investigation and seek
        changes                                   procedures                 advice from the relevant
                                                                             professional body

     Monitor situation                                                       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
```